

COMMONWEALTH OF MASSACHUSETTS.

APPEALS COURT

BRISTOL COUNTY

No. 2015-P-0558

COMMONWEALTH

V.

ADALBERTO MARTINEZ

BRIEF AND RECORD APPENDIX FOR THE DEFENDANT
ON APPEAL FROM THE FALL RIVER COURT DIVISION
OF THE DISTRICT COURT DEPARTMENT

MICHELLE A. DAME, ESQUIRE
ATTORNEY FOR THE DEFENDANT
Goodhines Law Offices
175 State Street, Suite 400
Springfield, MA 01103
michelle.dame@hotmail.com
Office (413) 737-0101
Facsimile (413) 731-7935
BBO# 687383

August 2015

TABLE OF CONTENTS

| | |
|---|----------|
| TABLE OF AUTHORITIES..... | ii |
| ISSUE..... | 1 |
| STATEMENT OF THE CASE..... | 1 |
| STATEMENT OF THE FACTS..... | 3 |
| Search Warrant Application and Affidavit..... | 3 |
| Computers, the Internet, and Wireless Networks..... | 5 |
| Suppression Hearing..... | 7 |
| ARGUMENT | |
| I. THE MOTION JUDGE ERRED IN DENYING MARTINEZ'S MOTION TO SUPPRESS BECAUSE THE IP ADDRESS ALONE DID NOT PROVIDE A SUFFICIENT NEXUS TO BELIEVE EVIDENCE OF CHILD PORNOGRAPHY WOULD BE FOUND AT 231 SUNSET HILL..... | 8 |
| A. Probable cause standard..... | 8 |
| B. Under the Fourth Amendment, there needs to be more evidence tying a specific residence to child pornography, other than an IP address, before a search warrant can issue..... | 10 |
| C. Under Article Fourteen of the Massachusetts Declaration of Rights, there needs to be more evidence tying a specific residence to child pornography, beyond a mere IP address, before a search warrant can issue..... | 20 |
| CONCLUSION..... | 25 |
| RULE 16K CERTIFICATION..... | 25 |
| ADDENDUM..... | (Add./1) |
| RECORD APPENDIX..... | (R.A./1) |

TABLE OF AUTHORITIES

Cases

| | |
|--|----------|
| <u>Commonwealth v. Anthony,</u> 451 Mass. 59, (2008) | 10, 21 |
| <u>Commonwealth v. Byfield,</u> 413 Mass. 426 (1992) | 8 |
| <u>Commonwealth v. Canning,</u> No. SJC-11773 (Apr. 27, 2015) (unpublished) | 23 |
| <u>Commonwealth v. Cinelli,</u> 389 Mass. 197 (1983) | 10 |
| <u>Commonwealth v. Kaupp,</u> 453 Mass. 102 (2009) | 8, 9, 23 |
| <u>Commonwealth v. Kenney,</u> 449 Mass. 840 (2007) | 9, 22 |
| <u>Commonwealth v. Upton II,</u> 394 Mass. 363 (1985) | 9, 20 |
| <u>Commonwealth v. Walker,</u> 438 Mass. 246 (2002) | 9 |
| <u>Draper v. United States,</u> 358 U.S. 307 (1959) | 9 |
| <u>Illinois v. Gates,</u> 462 U.S. 213 (1983) | 11 |
| <u>United States v. Bynum,</u> 604 F.3d 161 (4th Cir. 2010) | 15 |
| <u>United States v. Carter,</u> 549 F.Supp.2d 1257 (D.Nev. 2008) | 13 |
| <u>United States v. Elbe,</u> 774 F.3d 885 (6th Cir. 2014) | 12 |
| <u>United States v. Gourde,</u> 440 F.3d 1065 (9th Cir. 2006) | 11 |

| | |
|---|--------|
| <u>United States v. Grant,</u> 218 F.3d 72 (1st Cir. 2000) | 16, 22 |
| <u>United States v. Greathouse,</u> 297 F.Supp.2d 1264 (D.Or. 2003) | 13, 18 |
| <u>United States v. Hay,</u> 231 F.3d 630 (9th Cir. 2000) | 17, 18 |
| <u>United States v. Meeks,</u> 290 Fed. Appx. 896 (6th Cir. 2008) | 14 |
| <u>United States v. Perez,</u> 484 F.3d 735 (2007) | 13, 16 |
| <u>United States v. Reibert,</u> No. 8:13CR107 (D.Neb. Jan. 27, 2015) (unpublished) .. | 19 |
| <u>United States v. Stults,</u> 575 F.3d 834 (8th Cir. 2009) | 13 |
| <u>United States v. Valley,</u> 755 F.3d 581 (7th Cir. 2014) | 12 |
| <u>United States v. Ventresca,</u> 380 U.S. 102 (1965) | 9 |
| <u>United States v. Vosburgh,</u> 602 F.3d 512 (3d Cir. 2010) | 12 |
| <u>United States v. Voustianiouk,</u> 685 F.3d 206 (2d Cir. 2012) | 14, 15 |
| <u>United States v. Wagers,</u> 452 F.3d 534 (6th Cir. 2006) | 19 |
| <u>White Buffalo Ventures LLC v. University of Texas,</u> 420 F.3d 366 (5th Cir. 2005) | 5 |

Statutes

| | |
|-------------------------|---|
| G.L. c. 272, §29B | 1 |
| G.L. c. 272, §29C | 1 |

Other Authorities

Joshua J. McIntyre,
*Balancing Expectations of Online Privacy: Why Internet
Protocol (IP Addresses) Should Be Protected as
Personally Identifiable Information*, DEPAUL L. REV. 895
(2011) 5, 7, 12

Ned Snow,
*Accessing the Internet Through the Neighbor's Wireless
Internet Connection: Physical Trespass in Virtual
Reality*, 84 NEB. L. REV. 1226 (2006)
..... 6, 7, 12, 15, 17, 23

Constitutional Provisions

United States Constitution

Fourth Amendment..... 9, 10, 11, 20

Massachusetts Declaration of Rights

Article Fourteen..... 9, 20, 21, 24

ISSUE

- I. Did the motion judge violate Martinez's state and federal constitutional rights in denying his motion to suppress where merely linking a specific IP address to child pornography did not provide a sufficient nexus to search for evidence of child pornography at the residence assigned to the IP address?

STATEMENT OF THE CASE

On August 28, 2013, Adalberto Martinez was arraigned in Fall River District Court, Docket No. 1232-CR-2700, and charged with distributing material of a child in a sexual act, in violation of G.L. c. 272, §29B; and possession of child pornography, in violation of G.L. c. 272, §29C. (R.A./7) (Add./2-5).¹

On January 13, 2014, the charge of distributing material of a child in a sexual act was nolle prossed. (R.A./1-6). On August 15, 2014, Martinez filed a motion to suppress evidence seized from a search pursuant to a warrant. (R/A./42-49). That same day,

¹ The abbreviations used in this brief are as follows: the record appendix is cited as (R.A./page); the trial transcript is cited as (Tr.volume-page); the motion to suppress transcript is cited as (Mot.Tr.volume-page); the addendum is cited as (Add./page).

the suppression motion was heard in Fall River District Court. (Finnerty, J). The motion was denied on August 18, 2014. (R.A./42).

On November 12 and November 13, 2014, Martinez was tried before a judge with Judge Kevin J. Finnerty presiding. At the close of the Commonwealth's case, Martinez's oral Motion for Required Finding of Not Guilty was denied. (Tr.II-10-11). The jury convicted Martinez for possession of child pornography.

Martinez was sentenced to two and one half (2 ½) years in the house of correction, one (1) year to serve, the balance of eighteen (18) months suspended for a period of five (5) years of probation subject to the following conditions: registration with the Sex Offender Registry Board, no unsupervised contact with children under the age of sixteen (16), no volunteer activities involving children under the age of sixteen (16), no residing with children under the age of sixteen (16) except his own, and any supervised contact with persons under the age of sixteen (16) only after notice to probation officer and disclosure to the adult responsible for the child, and monitored by GPS during this period. (Tr.II-70-71). The sentence was not to begin until after Martinez's completion of

his current sentence on Bristol Superior Court Docket 1400405. (Tr.II-70). He filed a notice of appeal on November 18, 2014. (R/A./50-51) The case was entered in this Court on April 23, 2015.

STATEMENT OF THE FACTS

Search Warrant Application and Affidavit²

On March 9, 2012, Sergeant Michael Hill of the Massachusetts State Police Internet Crimes Against Children (ICAC) Task Force downloaded files containing child pornography from the Internet Protocol (IP) address 65.96.142.191. Through a subpoena, he received the following subscriber information for that address: Subscriber Name: Angel Martinez, Service Address: 231 Sunset Hill, Fall River, MA 02724-3753. Hill learned nothing from the subpoena that connected the defendant, Adalberto Martinez, to the IP address.

Hill advised the Fall River Police Department of this discovery on March 22, 2012, and the investigation was assigned to Detective Steven Washington. In the beginning of April, Washington went to 231 Sunset Hill and saw it was part of the Sunset

² The search warrant, search warrant application, and affidavit are part of the record appendix. (R.A./8-41).

Hill Housing Development. He verified 231 Sunset Hill was occupied by Maria Avilez, the mother of Angel Martinez. Angel Martinez is Adalberto Martinez's cousin. (Tr.I-62).

In the application for a search warrant, Washington relied on his training and experience to aver the following: (1) those who possess and/or disseminate child pornography "have an interest...in the sexual activity of children...[and] are likely to keep secreted, but readily at hand, sexually explicit visual images depicting children; (2) people "trading in, receiving, distributing or possessing of images or movies involving child pornography will make copies of those files on their computer's hard drive or other removable media;" (3) "even if a user deleted the files, they still may be recoverable by a trained computer forensic examiner;" (4) people involved with the exploitation of children "often communicate with others through correspondence or other documents...which could lead to identify the origin of these images;" (5) those with a sexual interest in children with access to the Internet "will conduct searches for child pornography and child sex stories on the Internet;" (6) "files related to the

exploitation of children found on computers are usually obtained from the Internet using application software;" and (7) "computers used to access the Internet usually contain files, logs, or file remnants...[tending] to show ownership of the computer as well as ownership and use of Internet service accounts." (R.A./16-17).

Based on this information, Washington applied for, and received, a search warrant for 231 Sunset Hill in Fall River to search for evidence relating to child pornography.

Computers, the Internet, and Wireless Networks

Computers and other devices accessing the Internet are assigned an Internet Protocol, or IP address. Joshua J. McIntyre, *Balancing Expectations of Online Privacy: Why Internet Protocol (IP Addresses) Should Be Protected as Personally Identifiable Information*, DEPAUL L. REV. 895, 902 (2011) (R.A./64).

"In essence an IP address identifies a single computer; that computer might be an entry point into an internal network." White Buffalo Ventures LLC v. University of Texas, 420 F.3d 366, 369 n.6 (5th Cir. 2005). A computer can be either a "stand alone" computer or a "networked computer." (R.A./26). A

"stand alone" computer is one that is isolated from, or not attached to any other computer. (R.A./26). This type of computer is becoming rarer in today's "high tech interconnected world." (R.A./26).

A "networked computer" is one that is connected to, attached to, or can communicate with other computers or hosts. (R.A./26). It consists of one or more stand alone computers which have the ability to communicate with each other. (R.A./31). Today, more and more people have small networks in their homes allowing two or more computers to share an Internet connection. (R.A./31). One way computers on the same network can share an Internet connection is through a wireless network card, which allows computers to connect to each other via the radio spectrum, the same way a cordless phone allows a user to move around with a telephone without it being plugged into anything. (R.A./31).

Wireless networks allow "computers within a local geographic area to share information without being connected by wires." Ned Snow, *Accessing the Internet Through the Neighbor's Wireless Internet Connection: Physical Trespass in Virtual Reality*, 84 NEB. L. REV. 1226, 1231 (2006) (R.A./87). Wi-Fi radio signals

originate from the Wi-Fi router which "transmits data between computers within the network, and between a modem that is connected to the Internet and a computer within the network." Id. Routers are capable of transmitting signals over a range of, on average, about 300 feet. Id. at 1232. Therefore, data can be transmitted between computers in separate buildings, and a neighbor of a Wi-Fi operator would be able to access the wireless network. Id. Additionally, the newest cell phones have the ability to access the Internet, allowing even easier Internet access.

(R.A./29). A Wi-Fi operator could prevent outsiders from accessing the network by setting up a password, but most do not do this, allowing anyone within range to access the network. Snow, supra p.6 at 1234 (R.A/87).

Any outsider who accesses the network would be linked to the IP address assigned to that network. See McIntyre, supra p.5 at 897 n.24 ("If multiple users access the Internet via the same subscriber account, the IP address will likely identify all of their Internet traffic and will not, therefore, be perfectly linked to any individual user") (R.A./72).

Suppression Hearing

Martinez filed a motion to suppress arguing the search warrant affidavit did not provide probable cause. (R.A./42-49). On August 15, 2014, this motion was heard in front of Judge Kevin J. Finnerty. Martinez argued the IP address was not enough to connect evidence of the crime to a specific address given the prevalence of wireless internet connections. (Mot.Tr.I-4-5). The Commonwealth even admitted there is always the possibility that someone sitting outside the residence could download child pornography if there was an open wireless network. (Mot.Tr.I-12-13). Judge Finnerty denied this motion three days later. (R.A./42). It is this decision Martinez now appeals.

ARGUMENT

- I. THE MOTION JUDGE ERRED IN DENYING MARTINEZ'S MOTION TO SUPPRESS BECAUSE THE IP ADDRESS ALONE DID NOT PROVIDE A SUFFICIENT NEXUS TO BELIEVE EVIDENCE OF CHILD PORNOGRAPHY WOULD BE FOUND AT 231 SUNSET HILL.

A. Probable cause standard.

"A search warrant may issue only on a showing of probable cause." Commonwealth v. Kaupp, 453 Mass. 102, 110 (2009), citing Commonwealth v. Byfield, 413 Mass. 426, 28 (1992). Probable cause exists to search if "the facts contained in the affidavit and reasonable inferences that may be drawn from them, [are]

sufficient for the magistrate to conclude that the items sought are related to the criminal activity under investigation and that they reasonably may be expected to be located in the place to be searched at the time the search warrant issues.'" Commonwealth v. Kenney, 449 Mass. 840, 845 (2007), quoting Commonwealth v. Walker, 438 Mass. 246, 249 (2002) (emphasis added).

The Massachusetts Supreme Judicial Court has expressly stated Article Fourteen of the Massachusetts Declaration of Rights "provides more substantive protection to criminal defendants" in determining probable cause than the Fourth Amendment. Commonwealth v. Upton II, 394 Mass. 363, 373-74 (1985) (rejecting totality of the circumstances test). While probable cause "'deal[s] with probabilities,'" Kaupp, 453 Mass. at 110, quoting Draper v. United States, 358 U.S. 307, 313 (1959), and the "affidavit 'should be interpreted in a common sense and realistic fashion,'" Kaupp, 453 Mass. at 111, quoting United States v. Ventresca, 380 U.S. 102, 108 (1965), a "'[s]trong suspicion to suspect is not adequate'" in finding probable cause. Kaupp, 453 Mass. at 111, quoting Upton II, 394 Mass. at 370.

To find probable cause, there must be a nexus between the type of evidence sought and the place to be searched. Commonwealth v. Anthony, 451 Mass. 59, 70 (2008). "'The nexus may be found in the type of crime, the nature of the...items [sought], the extent of the suspect's opportunity for concealment, and normal inferences as to where a criminal would be likely to hide [items of the sort sought].'" Id., quoting Commonwealth v. Cinelli, 389 Mass. 197, 213 (1983). In the present case, merely linking child pornography to an IP address registered to 231 Sunset Hill, did not provide a sufficient nexus between child pornography and 231 Sunset Hill. Without any further incriminating information, probable cause did not exist to believe evidence of child pornography would be found at 231 Sunset Hill, and the denial of Martinez's motion to suppress was a violation of his state and federal Constitutional rights.

B. Under the Fourth Amendment, there needs to be more evidence tying a specific residence to child pornography, other than an IP address, before a search warrant can issue.

"[Fourth Amendment rights]...are not mere second-class rights but belong in the catalog of indispensable freedoms." Illinois v. Gates, 462 U.S.

213, 274 (1983) (Brennan, dissenting) (citation omitted). "[F]or most people, their computers are their most private spaces." United States v. Gourde, 440 F.3d 1065, 1077 (9th Cir. 2006) (Kleinfeld, dissenting). Justice Kleinfeld explained there are many secrets kept on a person's computer, "most legal, some embarrassing, and some potentially tragic in their implications for loose liberality in allowing search warrants." Id. Seizing a computer which is shared by a family may have consequences unrelated to law enforcement, such as "confiscat[ing] a professor's book, a student's almost completed Ph.D. thesis, or a business's accounts payable and receivable." Id. at 1078.

"The privacy of computers is too important to let it be eroded by sexual disgust." Id. Because of this, it is clear to obtain a search warrant for computers at a particular residence, the Fourth Amendment demands establishing a nexus between child pornography and that residence, and this nexus cannot be met by merely stating an IP address registered to that residence is linked to child pornography.

While IP addresses are undoubtedly relevant in locating suspects involved with child pornography, if

a person has a wireless Internet connection, more than one computer can be connected to the single IP address and these computers could be located outside the residence. See McIntyre, supra p.5 at 897 n.24 ("If multiple users access the Internet via the same subscriber account, the IP address will likely identify all of their Internet traffic and will not, therefore, be perfectly linked to any individual user") (R.A./72); Snow, supra p.6 at 1232 (explaining data can be transmitted between separate buildings) (R.A./87). Because of this, there needs to be some further investigation, such as confirming the subscriber to the IP address actually resides at the residence attached to the IP address. See e.g., United States v. Elbe, 774 F.3d 885, 888 (6th Cir. 2014) (agent drove by residence linked to IP address and saw person matching suspect's picture on the porch using a computer); United States v. Valley, 755 F.3d 581, 586 (7th Cir. 2014) (public records check confirmed subscriber of IP address lived at the listed residence); United States v. Vosburgh, 602 F.3d 512, 518 (3d Cir. 2010) (steps were taken to confirm subscriber of IP address lived at the listed residence and lived there alone); United States v. Stults, 575

F.3d 834, 838 (8th Cir. 2009) (using LexisNexis, a postal service mail delivery check, and a motor vehicle registration check, investigators confirmed the defendant was the resident of the address subscribed to the IP address); United States v. Carter, 549 F.Supp.2d 1257, 1261 (D.Nev. 2008) (public records check, DMV check, and power company check, all confirmed IP subscriber lived at listed residence); United States v. Perez, 484 F.3d 735, 738 (2007) (a public records check, utilities company check, and an internet white pages check all indicated subscriber of IP address lived at the listed residence); United States v. Greathouse, 297 F.Supp.2d 1264 (D.Or. 2003) (investigators contacted DMV and various utilities to confirm subscriber of IP address owned listed residence and also observed his vehicle parked in the driveway).

In this case, investigators were not able to confirm the subscriber of the IP address, Angel Martinez, resided at 231 Sunset Hill. All that was learned through subsequent investigation was Maria Avilez lived at this residence. (R.A./16).

There is always the danger the person subscribed to the IP address does not live at the residence

listed. See United States v. Voustianiouk, 685 F.3d 206, 209-10 (2d Cir. 2012) (IP address was assigned to defendant at Apartment 1, but upon executing the warrant, investigators learned he lived on the second floor); United States v. Meeks, 290 Fed. Appx. 896, 898 (6th Cir. 2008) (investigators tracked IP address to subscriber, but while the subscriber paid for the Internet service, it was provided to another residence where her son lived).

While the Second Circuit in Voustianiouk said discovering the subscriber no longer lived at the listed residence may not necessarily invalidate the warrant, this is only where "the current resident continue[s] to pay for Internet service but had neglected to change the account holder's name." 685, F.3d at 213 (emphasis added). Without first attempting to confirm the IP address subscriber still resides at the residence attached to the IP address, warrants may be issued and executed to search a completely innocent person's home. See Voustianiouk, 685 F.3d at 212 ("if [the defendant] had not been home or had not answered the building's front door on the morning of the search, the agents might have very well entered and searched the first-floor apartment, which we have no

reason to believe was anything other than an innocent person's home").

Again, investigators in this case did not confirm Angel Martinez lived at 231 Sunset Hill, only that his mother did. (R.A./16). In addition, there is nothing in the record to suggest when the search warrant was executed, investigators learned Angel had moved out, and his mother still paid for the Internet service without changing the account name. Without this, there was not probable cause to search the residence. See Voustianiouk, 685 F.3d at 213 (explaining discovering the subscriber no longer lived at the listed residence may not necessarily invalidate the warrant if "the current resident continue[s] to pay for the Internet services but had neglected to change the account holder's name").

There is also the danger a subscriber to the Internet has an unsecured wireless connection, making it possible for any number of people to access the network outside of the residence. See Snow, supra p.6 at 132-34 (as most Wi-Fi operators do not set up a password for their network, anyone within range could access the network) (R.A./87). Contrast United States v. Bynum, 604 F.3d 161, 163 (4th Cir. 2010)

(investigators had information suspect was using a phone-based dial up service). The Fifth Circuit has acknowledged the possibility that transmissions may occur outside of the residence to which the IP address is assigned, but that it "remained likely" the source of transmission came from inside that residence. Perez, 484 F.3d at 740. However, the Fifth Circuit improperly compared an Internet connection to a screenname. Id. at 740 n.2. Using a screen name, or any other password protected account, requires the user to know the password associated with that account. United States v. Grant, 218 F.3d 72, 75 (1st Cir. 2000). Where there is "no evidence suggesting that on any given occasion, the user is not likely in fact to be the registrant," probable cause will still exist. Id. Further, investigators in Perez were able to confirm the subscriber resided at the residence associated with the IP address, strengthening the probable cause argument. 484 F.3d at 740.

In this case, investigators had no reason to believe the IP address in question was part of a dial-up service. If this was an unsecured wireless network, which was not password protected, anyone could have accessed the IP address, and could have done so

outside the residence. See Snow, supra p.6 at 132-34 (as most Wi-Fi operators do not set up a password for their network, anyone within range could access the network, including neighbors) (R.A./87). Even if it was a secure wireless network, and was password protected, while there may be reason to believe Angel Martinez was aware of the password, since he was the subscriber, there was no reason to believe he resided at 231 Sunset Hill. Therefore he could have been accessing the Internet outside of the residence.

Washington was on notice this IP address was likely a wireless connection, and could have been accessed by people outside the residence, as he observed 231 Sunset Hill was part of a housing development. (R.A./16). This case is similar to United States v. Hay, involving a search warrant on a college campus. 231 F.3d 630, 632 (9th Cir. 2000). There, investigators were able to track child pornography to an IP address associated with the University of Washington campus, and then specifically to the apartment which was assigned to the defendant. Id. An investigation revealed a substantial amount of additional evidence, besides the IP address, supporting probable cause to believe these images

would be found on the suspect's computer in his apartment. Id. at 632-34. During an undercover phone call, the defendant in Hay admitted he owned a computer, kept it in his apartment, and was the only one who used that computer. Id. He also admitted he used the University as his Internet Service Provider. Id. at 633. There was also evidence of the Hay defendant's extreme interest in young children through a website he maintained describing his extensive contact with children. Id. at 632, 634.

While a college campus is different from a single family residence where investigators may believe they are focusing on a single computer inside that residence, see Greathouse, 297 F.Supp.2d at 1271, the fact 231 Sunset Hill is part of a housing development is significant. (R.A./16). Because a housing development is comprised of housing units more akin to a college campus environment than a neighborhood of freestanding single family homes, probable cause is not established. This is so especially since investigators were unable to confirm Angel Martinez, the subscriber of the IP address, actually lived at 231 Sunset Hill. Contrast Greathouse, 297 F. Supp. at 1271 (by tracing the username, by checking ISP

records, and confirming the identity with DMV and utility records, there was probable cause to believe a computer located within the residence contained child pornography).

"In the Eighth Circuit, for the purposes of determining whether probable cause exists to search a computer, an IP address assigned to a specific user at the time illegal internet activity associated with that IP address occurs is a sufficient basis to find a nexus between the unlawful use of the internet at that IP address and a computer possessed by the subscriber assigned to that address." United States v. Reibert, No. 8:13CR107 (D.Neb. Jan. 27, 2015) (unpublished) (R.A./53). See also United States v. Wagers, 452 F.3d 534, 540 (6th Cir. 2006) (evidence connected the defendant, his IP address, his home and his computer to the offense).

While investigators may have connected the IP address in this case to the offense of child pornography, they were unable to connect anything else. There was no confirmation Angel Martinez lived at 231 Sunset Hill, no confirmation he owned a computer, and no confirmation that computer was used exclusively in 231 Sunset Hill. Further, while

investigators may have been able to search a computer in the possession of Angel Martinez, the subscriber, they were not authorized to search the computer in the possession of a third party. It is clear, the Fourth Amendment requires more evidence, other than an IP address, to establish probable cause to search a specific residence for child pornography. As a result, the denial of Martinez's motion to suppress was error, in violation of his Fourth Amendment rights.

C. Under Article Fourteen of the Massachusetts Declaration of Rights, there needs to be more evidence tying a specific residence to child pornography, beyond a mere IP address, before a search warrant can issue.

The Massachusetts Supreme Judicial Court has never relied on an IP address alone to support a finding of probable cause to search the physical address associated with that IP address. In fact, it appears this specific issue has never been before the Court. However, as Article Fourteen "provides more substantive protection to criminal defendants than does the Fourth Amendment in the determination of probable cause," it is likely more would be required. Upton II, 394 Mass. at 373. Since the Fourth Amendment requires more than an IP address alone to support a

finding of probable cause, see supra pp. 10-20, Article Fourteen certainly cannot require less.

In cases where the SJC has addressed this issue, its decisions suggest a much more substantial factual basis must support a finding of probable cause to search a private residence for a computer containing child pornography.

In Anthony, 451 Mass. at 60-61, an investigation revealed the defendant threatened a twelve (12) year old girl into sending sexually explicit pictures of herself. The Supreme Judicial Court held there was probable cause to search the defendant's storage locker for five (5) reasons: (1) 3 years prior he had pled guilty to charges involving possession of child pornography and was not supposed to use computers pursuant to probation, but admitted he did; (2) he used a computer to threaten a young girl into sending sexually explicit pictures; (3) he kept a list of websites appearing to relate to child pornography; (4) the police had information he owned as many as five (5) computers; and (5) he was homeless and rented a storage locker so it was reasonable to infer he was keeping his pornography in the only physical space under his control. Id. at 70-71.

In Kenney, 449 Mass. at 843, a woman contacted the police to tell them she had accessed the defendant's email and had found an email depicting child pornography. She further stated she had seen a computer in his house when she visited. Id. Police investigation was able to confirm the defendant lived at the address provided by the woman, and assigned to the email account, by seeing his vehicle in the driveway. Id. at 843-44.

The Kenney case differs from Martinez's case for two significant reasons. One, the account in Kenney was a password protected email account, while an IP address is not necessarily password protected. 449 Mass. at 843. See also Grant, 218 F.3d at 75 (explaining there is always reason to question whether an account is being used by the person who is registered to that account, but if it is password protected it requires at least the user know the password). Second, in Kenney, investigators confirmed the defendant lived at the residence assigned to the email address account. 449 Mass. at 844. See supra pp. 12-13. Investigators were never able to confirm Angel Martinez lived at 231 Sunset Hill.

The IP address assigned to 231 Sunset Hill could have been part of a wireless network where multiple computers from multiple locations were accessing the Internet. See Snow, supra p.6 at 1232 (explaining data can be transmitted between separate computers in separate buildings) (R.A./87). Just because one computer on a network contains child pornography, does not mean there is probable cause to believe all computers on that network contain child pornography. See Kaupp, 453 Mass. at 103-114 (no probable cause to search defendant's computer connected to school network even though another computer connected to the network had child pornography in its open share which was accessible to all network users). While it is possible an IP address may not be part of a wireless network, or may be password protected, it is not unreasonable to expect investigating officers to take some steps to confirm or dispel this. C.f. Commonwealth v. Canning, No. SJC-11773 (Apr. 27, 2015) (unpublished) (R.A./58-59) (when officers have probable cause to believe a person is growing marijuana in their home, it is possible they are registered to do so, and it is not an

"impossible burden" to expect them to confirm this)
(R.A./55-59).

When officers have probable cause to believe an IP address is linked to child pornography, before they are able to obtain a search warrant they should be required to establish (1) the IP address is not linked to a wireless internet service; (2) the IP address is linked to a wireless internet service, but it is a secure connection requiring a password; or (3) no one outside the residence would be accessing the network. Providing probable cause for one of those three things is not impossible, not unreasonable, and ensures that individuals' rights under Article Fourteen are protected.

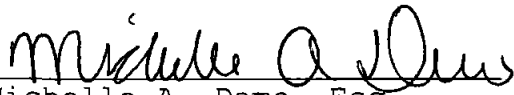
In this case, although investigators were able to link child pornography to an IP address registered to Angel Martinez, they were: 1) unable to confirm he lived at the location associated with the address; 2) unable to provide details about the type of Internet connection; and 3) unable to discern who would have been able to access this connection, and where they would have been able to do so. Accordingly, a search warrant should not have issued. Therefore, denying

Martinez's motion to suppress was error and violated his state constitutional rights.

CONCLUSION

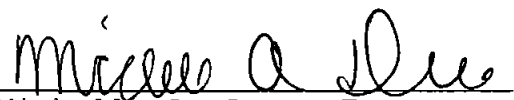
For all of the foregoing reasons, Martinez's conviction should be reversed.

Respectfully submitted,
ADALBERTO MARTINEZ


Michelle A. Dame, Esq.
Goodhines Law Offices
175 State Street, Suite 400
Springfield, MA 01103
michelle.dame@hotmail.com
Office (413) 737-0101
Facsimile (413) 731-7935
BBO# 687383

MASS. RULE OF APPELLATE PROCEDURE 16K CERTIFICATION

I, Michelle A. Dame, certify that this brief is in compliance with Mass. Rules of Appellate Procedure 16(a)(6), 16(e), 16(f), 16(h), 18, and 20.


Michelle A. Dame, Esq.
Goodhines Law Offices
175 State Street, Suite 400
Springfield, MA 01103
michelle.dame@hotmail.com
Office (413) 737-0101
Facsimile (413) 731-7935
BBO# 687383

ADDENDUM

TABLE OF CONTENTS

| | |
|--|--------|
| <u>Motion to Suppress Decision</u> | Add./1 |
| <u>United States Constitution</u> | |
| Fourth Amendment..... | Add./2 |
| <u>Massachusetts Declaration of Rights</u> | |
| Article Fourteen..... | Add./2 |
| <u>Massachusetts General Laws</u> | |
| G.L. c. 272, §29B..... | Add./2 |
| G.L. c. 272, §29C..... | Add./4 |

COMMONWEALTH OF MASSACHUSETTS

BRISTOL, ss.

DISTRICT COURT DEPARTMENT
FALL RIVER DIVISION
NO. 1232CR02700

COMMONWEALTH

v.

ADALBERTO MARTINEZ

MOTION TO SUPPRESS EVIDENCE

The defendant on the above-entitled matter moves, pursuant to Mass.R.Crim.P. 13, that this Honorable Court suppress from the use in evidence anything recovered as a result of a search and seizure made pursuant to Search Warrant number 9323 issued from Fall River District Court, including but not limited to, laptop computers. A copy of the warrant and affidavit are attached hereto.

The Defendant maintains that the issuance of a search warrant, the execution of the search warrant, the seizure of any items including any and all statements made by the Defendant, and the Defendant's arrest were illegal because:

- a. There was no probable cause to arrest the Defendant.
- b. The Affidavit in support of the Application for the Search warrant does not demonstrate probable cause on its face and is defective.
- c. The search warrant was improperly issued.
- d. The search preceded the arrest.
- e. There was no valid consent to search.
- f. There were no exigent circumstances which would authorize the warrantless search.
- g. The information in the affidavit is stale.

WHEREFORE, the Defendant maintains that his rights under the Fourth Amendment of the U.S. Constitution and Article Fourteen of the Declaration of Rights to the Constitution of the Commonwealth of Massachusetts have been violated.

After hearing, the court concludes that the Affidavit and accompanying exhibits in support of the Application for the search warrant for the premises at 231 Sunset Hill, Fall River, Ma. does provide probable

Adalberto Martinez,
By his attorney,

Add. /1

cause to believe contraband/evidence of specific criminal activity would be found there. The Defendant's motion is therefore DENIED. Summary 8-18-1

United States Constitution
Fourth Amendment

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Massachusetts Declaration of Rights
Article Fourteen

Every subject has a right to be secure from all unreasonable searches and seizures of his person, his houses, his papers, and all his possessions. All warrants, therefore, are contrary to this right, if the cause or foundation of them be not previously supported by oath or affirmation, and if the order in the warrant to a civil officer, to make search in suspected places, or to arrest one or more suspected persons, or to seize their property, be not accompanied with a special designation of the persons or objects of search, arrest, or seizure; and no warrant ought to be issued but in cases, and with the formalities, prescribed by the laws.

Massachusetts General Laws
G.L. c. 272, §29B

(a) Whoever, with lascivious intent, disseminates any visual material that contains a representation or reproduction of any posture or exhibition in a state of nudity involving the use of a child who is under eighteen years of age, knowing the contents of such visual material or having sufficient facts in his possession to have knowledge of the contents thereof, or has in his possession any such visual material knowing the contents or having sufficient facts in his possession to have knowledge of the contents thereof, with the intent to disseminate the same, shall be punished in the state prison for a term of not less than ten nor more than twenty years or by a fine of not less than ten thousand

nor more than fifty thousand dollars or three times the monetary value of any economic gain derived from said dissemination, whichever is greater, or by both such fine and imprisonment.

(b) Whoever with lascivious intent disseminates any visual material that contains a representation or reproduction of any act that depicts, describes, or represents sexual conduct participated or engaged in by a child who is under eighteen years of age, knowing the contents of such visual material or having sufficient facts in his possession to have knowledge of the contents thereof, or whoever has in his possession any such visual material knowing the contents or having sufficient facts in his possession to have knowledge of the contents thereof, with the intent to disseminate the same, shall be punished in the state prison for a term of not less than ten nor more than twenty years or by a fine of not less than ten thousand nor more than fifty thousand dollars or three times the monetary value of any economic gain derived from said dissemination, whichever is greater, or by both such fine and imprisonment.

(c) For the purposes of this section, the determination whether the child in any visual material prohibited hereunder is under eighteen years of age may be made by the personal testimony of such child, by the testimony of a person who produced, processed, published, printed or manufactured such visual material that the child therein was known to him to be under eighteen years of age, by testimony of a person who observed the visual material, or by expert medical testimony as to the age of the child based upon the child's physical appearance, by inspection of the visual material, or by any other method authorized by any general or special law or by any applicable rule of evidence.

(d) In a prosecution under this section, a minor shall be deemed incapable of consenting to any conduct of the defendant for which said defendant is being prosecuted.

(e) Pursuant to this section, proof that dissemination of any visual material that contains a representation or reproduction of sexual conduct or of any posture or exhibition in a state of nudity involving the use of a child who is under eighteen years of age was for a bona fide scientific, medical, or educational purpose for a bona fide school, museum, or library may be considered as evidence of a lack of lascivious intent.

G.L. c. 272, §29C

Whoever knowingly purchases or possesses a negative, slide, book, magazine, film, videotape, photograph or other similar visual reproduction, or depiction by computer, of any child whom the person knows or reasonably should know to be under the age of 18 years of age and such child is:

(i) actually or by simulation engaged in any act of sexual intercourse with any person or animal;

(ii) actually or by simulation engaged in any act of sexual contact involving the sex organs of the child and the mouth, anus or sex organs of the child and the sex organs of another person or animal;

(iii) actually or by simulation engaged in any act of masturbation;

(iv) actually or by simulation portrayed as being the object of, or otherwise engaged in, any act of lewd fondling, touching, or caressing involving another person or animal;

(v) actually or by simulation engaged in any act of excretion or urination within a sexual context;

(vi) actually or by simulation portrayed or depicted as bound, fettered, or subject to sadistic, masochistic, or sadomasochistic abuse in any sexual context; or

(vii) depicted or portrayed in any pose, posture or setting involving a lewd exhibition of the unclothed

genitals, pubic area, buttocks or, if such person is female, a fully or partially developed breast of the child; with knowledge of the nature or content thereof shall be punished by imprisonment in the state prison for not more than five years or in a jail or house of correction for not more than two and one-half years or by a fine of not less than \$1,000 nor more than \$10,000, or by both such fine and imprisonment for the first offense, not less than five years in a state prison or by a fine of not less than \$5,000 nor more than \$20,000, or by both such fine and imprisonment for the second offense, not less than 10 years in a state prison or by a fine of not less than \$10,000 nor more than \$30,000, or by both such fine and imprisonment for the third and subsequent offenses.


A prosecution commenced under this section shall not be continued without a finding nor placed on file.

The provisions of this section shall not apply to a law enforcement officer, licensed physician, licensed psychologist, attorney or officer of the court who is in possession of such materials in the lawful performance of his official duty. Nor shall the provisions of this section apply to an employee of a bona fide enterprise, the purpose of which enterprise is to filter or otherwise restrict access to such materials, who possesses examples of computer depictions of such material for the purposes of furthering the legitimate goals of such enterprise.

RECORD APPENDIX

TABLE OF CONTENTS

| | |
|---|---------|
| DOCKET | R.A./1 |
| COMPLAINT..... | R.A./7 |
| SEARCH WARRANT..... | R.A./8 |
| APPLICATION FOR SEARCH WARRANT..... | R.A./10 |
| AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT..... | R.A./11 |
| DEFENDANT'S MOTION TO SUPPRESS EVIDENCE..... | R.A./42 |
| MOTION TO SUPPRESS EVIDENCE DECISION..... | R.A./42 |
| NOTICE OF APPEAL | R.A./50 |
| <u>UNITED STATES V. REIBERT</u> , No. 8:13CR107 (D.Neb. Jan. 27, 2015) (unpublished)..... | R.A./52 |
| <u>COMMONWEALTH V. CANNING</u> , No. SJC-11773 (Apr. 27, 2015) (unpublished)..... | R.A./55 |
| JOSHUA J. MCINTYRE, <i>BALANCING EXPECTATIONS OF ONLINE PRIVACY: WHY INTERNET PROTOCOL (IP ADDRESSES) SHOULD BE PROTECTED AS PERSONALLY IDENTIFIABLE INFORMATION</i> , DEPAUL L. REV. 895, 902 (2011)..... | R.A./63 |
| NED SNOW, <i>ACCESSING THE INTERNET THROUGH THE NEIGHBOR'S WIRELESS INTERNET CONNECTION: PHYSICAL TRESPASS IN VIRTUAL REALITY</i> , 84 NEB. L. REV. 1226, 1231 (2006)..... | R.A./86 |

| | | | | | | | | | |
|--|----------------|---|--|---|--|---|-----------------|--|--|
| CRIMINAL DOCKET | | DOCKET NUMBER 1232CR002700 | | NO. OF COUNTS 2 | | Trial Court of Massachusetts District Court Department | |  | |
| DEFENDANT NAME AND ADDRESS Adalberto Martinez 57 Bates St. Fall River, MA 02724 | | | | DOB 07/28/1986 | | GENDER Male | | COURT NAME & ADDRESS Fall River District Court Fall River Justice Center 186 South Main Street Fall River, MA 02721 | |
| | | | | DATE COMPLAINT ISSUED 05/09/2012 | | | | | |
| | | | | PRECOMPLAINT ARREST DATE | | | | | |
| FIRST FIVE OFFENSE COUNTS | | | | | | | | | |
| COUNT | | CODE | | OFFENSE DESCRIPTION | | | | OFFENSE DATE | |
| 1 | | 272/29B/B | | CHILD IN SEXUAL ACT, DISTRIB MATERIAL OF c272 §29B(b) | | | | 03/09/2012 | |
| 2 | | 272/29C/A | | CHILD PORNOGRAPHY, POSSESS c272 §29C | | | | 03/09/2012 | |
| WARRANT | | | | | | | | | |
| DEFENSE ATTORNEY Fagan | | | | OFFENSE CITY/TOWN Fall River | | POLICE DEPARTMENT Fall River PD | | | |
| DATE & JUDGE | | DOCKET ENTRY | | | | DATE & JUDGE | | FEES IMPOSED | |
| AUG 28 2012 | | <input type="checkbox"/> Attorney appointed (SJC R. 3:10) <input type="checkbox"/> Atty denied & Deft. Advised per 211 D §2A <input type="checkbox"/> Waiver of Counsel found after colloquy HEA w/o Terms of release set: <input type="checkbox"/> PR <input type="checkbox"/> Bail BAIL <input type="checkbox"/> See Docket for special condition <input type="checkbox"/> Held (276 §58A) w/o RET. <input checked="" type="checkbox"/> Potential of bail revocation (276 §58) <input type="checkbox"/> Right to bail to review (276 §58) <input type="checkbox"/> Right to drug exam (111E § 10) <input checked="" type="checkbox"/> Arraigned and advised: <input type="checkbox"/> Waiver of jury found after colloquy <input type="checkbox"/> Does not waive <input checked="" type="checkbox"/> Advised of right to jury trial <input type="checkbox"/> Advised of trial rights as pro se (Dist. Ct. Supp.R.4) <input type="checkbox"/> Advised of right of appeal to Appeals Ct. (M.R. Crim P.R. 28) | | | | AUG 28 2012 | | Counsel Fee (211D § 2A(12)) <input checked="" type="checkbox"/> WAIVED Counsel Contribution (211D § 2) <input type="checkbox"/> WAIVED Default Warrant Fee (276 § 30(1)) <input type="checkbox"/> WAIVED Default Warrant Arrest Fee (276 § 30(12)) <input type="checkbox"/> WAIVED Probation Supervision Fee (276 § 87A) <input type="checkbox"/> WAIVED Ball Order Forfeited 100 min then upon release in HOU in | |
| | | | | | | 11/3/12 | | | |
| | | | | | | | | | |
| | | | | WARRANT ISSUE | | | | | |
| SCHEDULING HISTORY | | | | | | | | | |
| NO. | SCHEDULED DATE | EVENT | RESULT | | | JUDGE | TAPE START/STOP | | |
| 1 | 8/28/12 | Arr | <input type="checkbox"/> Held <input type="checkbox"/> Not Held but Event Resolved <input type="checkbox"/> Cont'd HABE TO NORFOLK ISSUED | | | | | | |
| 2 | | | <input type="checkbox"/> Held <input type="checkbox"/> Not Held but Event Resolved <input type="checkbox"/> Cont'd FAFED + MAILED | | | | | | |
| 3 | | | <input type="checkbox"/> Held <input type="checkbox"/> Not Held but Event Resolved <input type="checkbox"/> Cont'd ALSO HAS A SUP CT WARRANT | | | | | | |
| 4 | | | <input type="checkbox"/> Held <input type="checkbox"/> Not Held but Event Resolved <input type="checkbox"/> Cont'd BRIEFING SUP CT NOTIFIED | | | | | | |
| 5 | | | <input type="checkbox"/> Held <input type="checkbox"/> Not Held but Event Resolved <input type="checkbox"/> Cont'd AS TO THIS DATE. | | | | | | |
| 6 | | | <input type="checkbox"/> Held <input type="checkbox"/> Not Held but Event Resolved <input type="checkbox"/> Cont'd | | | | | | |
| 7 | | | <input type="checkbox"/> Held <input type="checkbox"/> Not Held but Event Resolved <input type="checkbox"/> Cont'd | | | | | | |
| 8 | | | <input type="checkbox"/> Held <input type="checkbox"/> Not Held but Event Resolved <input type="checkbox"/> Cont'd | | | | | | |
| 9 | | | <input type="checkbox"/> Held <input type="checkbox"/> Not Held but Event Resolved <input type="checkbox"/> Cont'd | | | | | | |
| 10 | | | <input type="checkbox"/> Held <input type="checkbox"/> Not Held but Event Resolved <input type="checkbox"/> Cont'd | | | | | | |
| APPROVED ABBREVIATIONS ARR = Arraignment PTH = Pretrial hearing DCE = Discovery compliance & jury selection BTR = Bench trial JTR = Jury trial PCH = Probable cause hearing MOT = Motion hearing SRE = Status review SRP = Status review of payments FAT = First appearance in jury session SEN = Sentencing CWF = Continuance without finding scheduled to terminate PRO = Probation scheduled to terminate DFTA = Defendant failed to appear & was defaulted WAR = Warrant issued WARD = Default warrant issued WR = Warrant or default warrant recalled PVH = probation revocation hearing. | | | | | | | | | |
| A TRUE COPY ATTEST: | | CLERK-MAGISTRATE / ASST CLERK X | | | | TOTAL NO. OF PAGES | | ON (DATE) | |

| CRIMINAL DOCKET DOCKET ENTRIES | | DEFENDANT NAME Adalberto Martinez | DOCKET NUMBER 1232CR002700 |
|-----------------------------------|---|--------------------------------------|-------------------------------|
| DATE | DOCKET ENTRIES | | |
| AUG 28 2013 | C-9/25/13-PTH-Mitt & Hake | | |
| SEP 25 2013 | C-10/23/13-PTH-Mitt & Hake (iss) Maryland County C.C. | | |
| 10/23/13 | { (Cannon 1) C 127273 PCH Qm #5 Mitt & Hake 30 Day Date waived | | |
| DEC 12 | Madeau - C-1-13-14-PTH over 1/2 objection Mitt (iss) | | |
| 1/13/14 | Dunq J - C-2/11/14-PTH-Mitt to issue (iss) | | |
| FEB 11 | Madeau - C-3/6/14-JT JURY OF Mitt (iss) | | |
| 3/5/14 | Motion to Continue granted | | |
| 4/2/14 | Finnerty J. (C) can't to 5/19/14 JT Motion to Cont - Allowed C-4-7-14-JSR Moorey Hake to issue | | |
| 4/7/14 | AFTER HEARING, BAIL IS SET IN THE AMOUNT OF \$10,000 CASH - 100,000 SURETY CONT 5/1/14 JT MITT ISSUED (FINNERTY O) | | |
| APR 29 | Hernon, J - C-6/2/14-JT - Mitt to issue Comm's Motion to Continue due to Police officer not available - Allowed over objected of J.C. - N/A Mitt (iss) 5/28/14 Motion to withdraw | | |

APPROVED ABBREVIATIONS

ARR = Arraignment PTM = Pretrial hearing DCE = Discovery compliance & jury selection BTR = Bench trial JTR = Jury trial PCH = Probable cause hearing MOT = Motion hearing SRE = Status review
SRP = Status review of payments FAT = First appearance in jury session SEN = Sentencing CWF = Continuance-without-finding scheduled to terminate PRO = Probation scheduled to terminate
DFTA = Defendant failed to appear & was defaulted WAR = Warrant issued WARD = Default warrant issued WR = Warrant or default warrant recalled PVH = probation revocation hearing.

| DOCKET CONTINUATION | | NAME OF CASE | DOCKET NUMBER |
|---------------------|--------------|---|---------------|
| | | Adelberto Martinez | 12-2700 |
| NO. | DATE | DOCKET ENTRIES | |
| | MAY 28, 2014 | Mooney, J - C- 6/26/14 - SEB - Cst. 2 | |
| | | A/C Motion to Withdraw - Allowed. | |
| | | Atty. Clone Appt. Mitt to issue (cos.) | |
| | 6/26/14 | Finnerty J DS No in funds - in COM | |
| | | Filed - Cst Allowed | |
| | | C to 7/18/14 BT → Mitt # (5) | |
| | JUL 18 2014 | Dunn C + 8/15/14 M (2) Mitt (SS) | |
| | 8/14/14 | Habe iss to mpc Cedar Junction faxed (C) | |
| | 8/15/14 | Finnerty hearing on motion to suppress - under advisement C 9/16/14 SK | |
| | | C/R (2) | |
| | 8/18/14 | Judge Finnerty After Hearing Motion Denied | |
| | 9/11/14 | attorney, Clone called and requested that the habe be not be issued for 9/16/14 | |
| | | he has spoken to his client and is waiving his client's appearance - habe is cancelled - 9/16/14 SK (lock up not filed) | |
| | SEP 16 2014 | Dunn, J - C- 11/12/14 - JT (A waives 30 days) | |
| | | Mitt's Habe from Walpole (JT) | |
| | 11/12/14 | Appt CPSC (att. Wallin) for W. Rott | |
| | CR 2 | Reinier Av. 5th amendment inv. | |
| | 11:30- | Motion to Sequester w/s allowed | |
| | | Motion to Exclude Hearsay 5th Denied | |
| | | Jury Sworn 1:15 pm | |
| | | A for ID - Computer Ex #1 - DISC | |
| | | B for ID - Computer | |
| | | C for ID - List | |
| | | Trial Suspended at 4:30 c 11/13/14 JT | |
| | | Finnerty | |

| NO. | DATE | DOCKET ENTRIES |
|-----|----------|--|
| | 11/13/14 | <p>Finney J. Thurgood Marshall continued start @ 9:23, end @</p> <p>~ DS Mo. In Union Permit the D to approach Comm's witness w/ evidence of Prior Conviction filed - ct. Allowed</p> <p>Comm rests @ 9:29</p> <p>~ DS oral mo. for Required Findings @ Close of Comm's Case DENIED D rests @ 9:31</p> <p>~ DS oral mo. for Required Findings of NGT @ close of all evidence DENIED</p> <p>~ Comm's oral mo. for "consummation of Crime" Charge / instruction DENIED Jury out @ 11:00 → 11:10 Guilty</p> <p><u>Sentence Continued:</u></p> <p>~ GPS monitor for 5 years</p> <p>→ <u>NIS</u> Suspended date of 11/13/21 is to be adjusted upon DS release from HCL's Sup. Fee is to be imposed for a period of 5 years upon DS release from HCL</p> <p>D signed Notice to Sex Offender from Welch J. D.C. Motion to withdraw - Allowed</p> <p>AS Motion of Notice to Appeal filed in court - Allowed</p> <p>AS Motion for Appointment of Appellate Counsel filed in court - Allowed</p> <p>11-18-14 notice of appeal filed by Atty Anthony Clune motion to withdraw and motion to appoint</p> |
| | | R A / 5 |

DOCKET
CONTINUATION

NAME OF CASE

Adalberto Martinez

DOCKET NUMBER

1232CR002700

NO.

DATE

DOCKET ENTRIES

appellate counsel allowed by Judge Welch
CPCS notified to assign counsel

| | | | | | |
|--|--------------------------------|------------------------------------|--------------------|--|--|
| CRIMINAL COMPLAINT ORIGINAL | | DOCKET NUMBER 1232CR002700 | NO. OF COUNTS 2 | Trial Court of Massachusetts District Court Department | |
| DEFENDANT NAME & ADDRESS Adalberto Martinez 57 Bates St. Fall River, MA 02724 | | | | COURT NAME & ADDRESS Fall River District Court Fall River Justice Center 186 South Main Street Fall River, MA 02721 (508)491-3200 | |
| DEFENDANT DOB 07/28/1986 | COMPLAINT ISSUED 05/09/2012 | DATE OF OFFENSE 03/09/2012 | ARREST DATE | | |
| OFFENSE CITY / TOWN Fall River | | OFFENSE ADDRESS | | NEXT EVENT DATE & TIME | |
| POLICE DEPARTMENT Fall River PD | | POLICE INCIDENT NUMBER 12-287WA | | NEXT SCHEDULED EVENT WARRANT | |
| OBTN | | | | ROOM / SESSION | |
| The undersigned complainant, on behalf of the Commonwealth, on oath complains that on the date(s) indicated below the defendant committed the offense(s) listed below and on any attached pages. | | | | | |

| COUNT | CODE | DESCRIPTION |
|-------|-----------|--|
| 1 | 272/29B/B | CHILD IN SEXUAL ACT, DISTRIB MATERIAL OF c272 §29B(b) <i>NP 1-13-14 MB</i> |

On 03/09/2012, with lascivious intent, did disseminate visual material that contained a representation or reproduction of an act that depicted, described or represented sexual conduct participated or engaged in by a child who was under eighteen years of age, knowing the contents of such visual material or having sufficient facts in his or her possession to have had knowledge of the contents thereof, or did have in his or her possession some such visual material knowing the contents or having sufficient facts in his or her possession to have had knowledge of the contents thereof, with the intent to disseminate the same, in violation of G.L. c.272, §29B(b).

NO DISTRICT COURT FINAL JURISDICTION IN ADULT SESSION; upon conviction, must register as a sex offender pursuant to G.L. c. 6, §§178C-178P; upon conviction, must register as a sex offender pursuant to G.L. c. 6, §§178C-178P.

| | | |
|---|-----------|--------------------------------------|
| 2 | 272/29C/A | CHILD PORNOGRAPHY, POSSESS c272 §29C |
|---|-----------|--------------------------------------|

On 03/09/2012 did knowingly purchase or possess a negative, slide, book, magazine, film, videotape, photograph or other similar visual reproduction, or depiction by computer, of a child whom the defendant knew or reasonably should have known to be under the age of 18 and who was: (1) actually or by simulation engaged in an act of sexual intercourse with a person or animal, or in an act of sexual contact involving the sex organs of the child and the mouth, anus or sex organs of the child and the sex organs of another person or animal, or in an act of masturbation, or in an act of excretion or urination within a sexual context; or (2) actually or by simulation portrayed as being the object of, or otherwise engaged in, an act of lewd fondling, touching, or caressing involving another person or animal; or (3) actually or by simulation portrayed or depicted as bound, fettered, or subject to sadistic, masochistic, or sadomasochistic abuse in a sexual context; or (4) depicted or portrayed in a pose, posture or setting involving a lewd exhibition of the unclothed genitals, pubic area; buttocks or, if such person is female, a fully or partially developed breast of the child; with knowledge of the nature or content thereof, in violation of G.L. c.272, §29C.

PENALTY: state prison not more than 5 years; or jail or house of correction not more than 2½ years; or not less than \$1000, not more than \$10,000 fine; or both such fine and imprisonment; cannot be continued without a finding or placed on file; upon conviction, must register as a sex offender pursuant to G.L. c. 6, §§178C-178P.

| | | |
|---|---|----------------|
| SIGNATURE OF COMPLAINANT <i>X</i> <i>Scall</i> | SWORN TO BEFORE CLERK-MAGISTRATE/ASST. CLERK/DEP. ASST. CLERK <i>X</i> <i>John C. O'Neil</i> | DATE 5/9/12 |
| NAME OF COMPLAINANT | A TRUE COPY ATTEST <i>X</i> <i>John C. O'Neil</i> | DATE 5/9/12 |

Notice to Defendant: 42 U.S.C. § 3796gg-4(e) requires this notice: If you are convicted of a misdemeanor crime of domestic violence you may be prohibited permanently from purchasing and/or possessing a firearm and/or ammunition pursuant to 18 U.S.C. § 922 (g) (9) and other applicable related Federal, State, or local laws.

SEARCH WARRANT

G.L. c. 276, §§ 1-7

TRIAL COURT OF MASSACHUSETTS
Second District



Fall River

COURT DEPARTMENT
DIVISION

SEARCH WARRANT DOCKET NUMBER

9323

TO THE SHERIFFS OF OUR SEVERAL COUNTIES OR THEIR DEPUTIES, ANY STATE POLICE OFFICER, OR ANY CONSTABLE OR POLICE OFFICER OF ANY CITY OR TOWN, WITHIN OUR COMMONWEALTH:

Proof by affidavit, which is hereby incorporated by reference, has been made this day and I find that there is PROBABLE CAUSE to believe that the property described below:

- ☐ has been stolen, embezzled, or obtained by false pretenses.
- ☒ is intended for use or has been used as the means of committing a crime.
- ☒ has been concealed to prevent a crime from being discovered.
- ☒ is unlawfully possessed or concealed for an unlawful purpose.
- ☒ is evidence of a crime or is evidence of criminal activity.
- ☐ other (specify) _____

YOU ARE THEREFORE COMMANDED within a reasonable time and in no event later than seven days from the issuance of this search warrant to search for the following property:

See Exhibit 2

☒ at

231 Sunset Hill, which is a housing development in the City of Fall River

which is occupied by and/or in the possession of: Angel Martinez 03/27/83 and Maria Avilez 08/17/45

☒ on the person or in the possession of:

Angel Martinez 03/27/83 and Maria Avilez 08/17/45

You ☒ are ☐ are not also authorized to conduct the search at any time during the night.

You ☐ are ☒ are not also authorized to enter the premises without announcement.

You ☒ are ☐ are not also commanded to search any person present who may be found to have such property in his or her possession or under his or her control or to whom such property may have been delivered.

YOU ARE FURTHER COMMANDED if you find such property or any part thereof, to bring it, and when appropriate, the persons in whose possession it is found before the

Fall River

Division of the

Second District

Court Department

DATE ISSUED

April 3, 2012

SIGNATURE OF JUSTICE, CLERK, MAGISTRATE OR ASSISTANT CLERK

X *[Signature]*

FIRST OR ADMINISTRATIVE JUSTICE

WITNESS: Gilbert J. Nadeau Jr.

PRINTED NAME OF JUSTICE, CLERK, MAGISTRATE OR ASSISTANT CLERK

Sharon E. Haggan

RETURN OF OFFICER SERVING SEARCH WARRANT

A search warrant must be executed as soon as reasonably possible after its issuance, and in any case may not be validly executed more than 7 days after its issuance. The executing officer must file his or her return with the court named in the warrant within 7 days after the warrant is issued. G.L. c. 276. §3A.

This search warrant was issued on 04/03/12 , and I have executed it as follows:
DATE

The following is an inventory of the property taken pursuant to this search warrant

- 1 1 HP G60-535DX Computer Notebook
- 2 Compaq Presario A900 Computer Notebook
- 3 _____
- 4 _____
- 5 _____
- 6 _____
- 7 _____
- 8 _____
- 9 _____
- 10 _____
- 11 _____
- 12 _____
- 13 _____
- 14 _____
- 15 _____
- 16 _____
- 17 _____
- 18 _____
- 19 _____
- 20 _____

(attach additional pages as necessary)

This inventory was made in the presence of Det. Thomas Chace

I swear that this inventory is a true and detailed account of all the property taken by me
on this search warrant.

R.A./9

SIGNATURE OF PERSON MAKING SEARCH

DATE AND TIME OF SEARCH

SWORN AND SUBSCRIBED TO BEFORE

PRINTED NAME OF PERSON MAKING SEARCH

TITLE OF PERSON MAKING SEARCH

DATE SWORN AND SUBSCRIBED TO

Det. Steven Washington

Detective

April 6, 2012

APPLICATION FOR SEARCH WARRANT

G.L.c. 276, §§ 1-7

TRIAL COURT OF MASSACHUSETTS



NAME OF APPLICANT

Second District

COURT DEPARTMENT

Detective Steven Washington

Fall River

DIVISION

POSITION OF APPLICANT

SEARCH WARRANT DOCKET NUMBER

Detective

I, the undersigned APPLICANT, being duly sworn, depose and say that:

1. I have the following information based upon the attached affidavit(s), consisting of a total of 8 pages, which is (are) incorporated herein by reference.

2. Based upon this information, there is PROBABLE CAUSE to believe that the property described below:

- ☐ has been stolen, embezzled, or obtained by false pretenses.
- ☒ is intended for use or has been used as the means of committing a crime.
- ☒ has been concealed to prevent a crime from being discovered.
- ☒ is unlawfully possessed or concealed for an unlawful purpose.
- ☒ is evidence of a crime or is evidence of criminal activity
- ☐ other (specify) _____

3. I am seeking the issuance of a warrant to search for the following property (describe the property to be searched for as particularly as possible):

See Exhibit 2

4. Based upon this information, there is also probable cause to believe that the property may be found (check as many as apply):

☒ at (identify the exact location or description of the place(s) to be searched):

231 Sunset Hill, which a housing development in the City of Fall River.

which is occupied by and/or in the possession of Angel Martinez 03/27/83 and Maria Avilez 08/17/45

☒ on the person or in the possession of (identify any specific person(s) to be searched):

Angel Martinez 03/27/83 and Maria Avilez 08/17/45

☒ on any person present who may be found to have such property in his or her possession or under his or her control or to whom such property may have been delivered.

THEREFORE, I respectfully request that the court issue a Warrant and order of seizure, authorizing the search of the above described place(s) and person(s), if any, to be searched, and directing that such property or evidence or any part thereof, if found, be seized and brought before the court, together with such other and further relief that the court may deem proper.

I ☐ have previously submitted the same application.

I ☒ have not previously submitted the same application.

PRINTED NAME OF APPLICANT

Detective Steven Washington

SIGNED UNDER THE PENALTIES OF PERJURY

X [Signature]
Signature of Applicant

SWORN AND SUBSCRIBED TO BEFORE

X [Signature]
Signature of Justice, Clerk-Magistrate or Assistant Clerk

4-372

Date

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

1. I, Detective Steven Washington, being duly sworn, depose and say:
2. Being part of the Fall River Police Department Major Crimes Division is a member of Massachusetts Internet Crimes Against Children (ICAC) that is comprised of Federal, State and Local Law Enforcement. The Task Force is responsible for conducting undercover online investigations, responding to complaints regarding children sexually exploited via the Internet, conducting community education programs and monitoring of the Internet for the bartering in child pornography. I have been a law enforcement officer for 17 years and a member of the Major Crimes Division for six years. During this time I have investigated numerous incidents of child abuse (including child sexual abuse) and child pornography. During this time I have received training in the field of child physical and sexual abuse as well as the use of the Internet by Sexual Offenders to seduce, entice and gain access to children for the purposes of sexual exploitation

~~I have conducted and participated in hundreds of investigations regarding child~~ exploitation on the Internet, as well as other investigations involving the use of a computer or computer systems. From my training and experience, I am familiar with the techniques and methods of operation used by individuals involved in criminal activity to conceal their activities from detection by law enforcement authorities. I have participated in investigations into the activities of individuals and groups involved in sexual assault, the use of the Internet to entice, seduce and gain access to children, endangering the welfare of a child, harassment and conspiracy. In addition, I have been involved in the preparation and execution of numerous search warrants.

As part of my duties I investigate violations of state law, including the online exploitation of children, particularly in relation to violations of Massachusetts General Law 272 Section 29B (A)(C) which criminalize, among other things, the possession, receipt and transmission of child pornography. I have gained experience in the conduct of such investigations through training in seminars, and classes. I have attended numerous computer crime conferences over the past six years.

3. This affidavit has attached hereto and incorporated herein by reference of the following attachments:
 - a. Exhibit 1: A seven (7) page document detailing peer to peer file sharing and the Ares Network provided by Sgt. Michael Hill.
 - b. Exhibit 2: An eleven (11) page document providing background information on computer systems.
 - c. Exhibit 3: A one (1) page biography of Sgt. Michael Hill's professional experience and training as an investigator and experience with peer to peer file sharing networks on the Internet.
 - d. Appendix A: A five (4)-page document detailing the items to be searched for

at the search location, 231 Sunset Hill in Fall River Massachusetts.

5. The facts establishing the grounds for my request to the court for the issuance of a search warrant are as follows:

On 03/22/12, Sgt. Michael Hill of the Massachusetts State Police Internet Crimes Against Children (ICAC) Task Force advised the Fall River Police Department that as a result of his responsibilities with the ICAC Task Force, he had conducted an investigation into the use of peer to peer file sharing programs on the Internet to possess and disseminate child pornography and that during the course of his duties he discovered a computer with an Internet Protocol (IP) address of 65.96.142.191 that had reported an association with at least one suspected child pornography file. As a result of this, Sgt. Michael Hill continued his investigation and subsequently downloaded digital files containing child pornography from a computer using IP address 65.96.142.191. The following is an excerpt from the report of Sgt. Michael Hill (*italicized*):

On 03/09/2012, I was conducting investigations into the use of Peer to Peer, hereinafter P2P, file sharing programs for the possession and distribution of child pornographic images and movies in violation of MGL Chapter 272 §§ 29B and MGL Chapter 272 §§ 29C. While conducting this investigation, I was connected to the Ares network (a public file sharing network which uses the Internet) using an Ares client software program installed on my computer. The investigation was documented, which included screen capture images at various stages of the investigation.

On 03/09/2012, working in an official capacity, I was connected to the Ares network through the internet using an Ares client program. On 03/09/2012 at approximately 1130 hrs (EST) I located a host computer on the Ares network that was recently reporting itself as sharing suspected child pornography files to the network. I observed this host computer to have an Internet Protocol (IP) address¹ of 65.96.142.191. Based on geographic mapping of this host IP address, I believed the associated computer to be located in Massachusetts. I reviewed the list of files that the host computer with public IP address 65.96.142.191 was recently reporting to the network that it had in its possession and displaying as available for sharing. This list consisted of ten (10) files, the majority of which had terms in the file names consistent with child pornography terms. I know that this list may not be all inclusive. The list of files that I did observe contained file attributes such as, file names, types, sizes, and SHA-1² hash values. The following is a sampling of the list of the file names and SHA-1 hash values recently reported to the Ares network from the host computer with public IP address

¹ Computers on the Internet identify each other by an Internet Protocol or IP address. IP addresses can assist law enforcement in finding a particular computer on the Internet. IP addresses can typically lead the law enforcement officer to a particular Internet service company and that company can typically identify the account that used the IP address to access the Internet.

² SHA-1 or Secure Hash Algorithm Version 1 is a file encryption method which may be used to produce a unique digital signature of a file. It is computationally infeasible (2^{160}) to find two different files that produce the same SHA-1 value. The Secure Hash Algorithm (SHA) was developed by the National Institute of Standards and Technology (NIST), along with the National Security Agency (NSA), for use with the Digital Signature Standard (DSS) as specified within the Secure Hash Standard (SHS). The United States of America has adopted the SHA-1 hash algorithm described herein as a Federal Information Processing Standard.

Search Warrant Affidavit for 231 Sunset Hill in Fall River Massachusetts

Page: 2 of 8

R.A./12

SW 4/3/12 JSH

65.96.142.191:

| File Name | SHA-1 |
|---|----------------------------------|
| webcam - vivi_morangulinho04 (brasileirinha 7)(brasíl ptbc pisc knabincj menina garola).avi | 5KNCHEMCKAXWXTG252ZGQC4IQVBJ4CNI |
| sdpa vaginitas de niãfãtas y bebães de 1 a 6 aãfãtos babij ptbc 2.wmv | 5GJCGQZMWNQXQFOLDHP2YCALWWWKLGZZ |
| niãfãta em el baãfãto posando.avi | RMW3QVQ2J5Y3PQGYNWL23FZW2NR50TV |
| | 58MSSRQHQZQW3ZPHW5QJ334GM2V6C4I |
| !new ptbc dark studio 10yro spread wide(2).avi | Z5KUC5K2DADD77BZMQENMV3LB2WDVGKT |
| sickcam sisters(2).avi | 63460CD5FR7YSVSSLRRPSPCIETA5TDFA |
| ptbc vicky - pumped girl 12 aãfãtos rãledinha na xoxotinha(2).mpg | EDREJNYJ3F30R4TENEIV7EZMW5PQCSWF |
| | V4EQ6AJH2UAGAYHTTSW33GC4YTHRND5Q |
| 10yr mandy all(2).avi | 7TVKVLHNUCTWUPM3XXULNDINGXJ06YY |
| | 77QWLDRVFIY3VFPDFLOCHM5EXTOUR4R |

On 03/09/2012 at approximately 1130 hrs (EST), using one of the features available in the Ares P2P client I was using, I determined that the user of this host computer located at IP address 65.96.142.191 had left the Ares client program configured to share files.

This officer has become familiar with some of the slang used by collectors of child pornography. Through my training and experience, I know that child pornography files are routinely named with some of the following terms, which are found in some of the files listed above: pthc, ptsc, and babyj. For example, I know through my training and experience that the term "pthc" means "pre-teen hardcore" and that "ptsc" means "pre-teen softcore". I also know that the letters "yr" following a numeric value, such as, 10yo or 11yo, or 11yr often indicate an age of 10 years old or 11 years old.

The list of file names that I observed and their associated SHA1 values included a video file with the SHA-1 value of 5KNCHEMCKAXWXTG25Z2GQC4IQVBJ4CNJ which had a file name of "webcam - vivi_moranginho04 (brasileirinha 7)(brasil pthc ptsc knabinoj menina garota).avi". On 03/09/2012 at approximately 11:30:50 hrs (EST), I requested the above video file having SHA1 value of 5KNCHEMCKAXWXTG25Z2GQC4IQVBJ4CNJ from the computer with host IP address 65.96.142.191. I was able to connect directly to the computer with host IP address 65.96.142.191 and download this complete file directly from the computer with host IP address 65.96.142.191. The download process ended on 03/09/2012 at approximately 11:33:02 hrs (EST). I viewed the video file and would describe it as a six minute and forty-eight second web cam type video depicting a young prepubescent female that appears approximately 8 to 10 years old. The female removes her shirt exposing her breasts. She then pulls down her pants and underwear exposing her vagina. She is observed masturbating her vagina. The female is then observed inserting a pencil type object into her anus. This video, based on my training and experience, appears to be child pornography in violation of MGL Chapter 272 §§ 29B and 29C. I know that the Ares network download process actually makes a copy of the selected file, leaving the original file on the host computer. Additionally, during the download process I observed the host computer located at IP address 65.96.142.191 to have an Ares version 3.1.7.3042 client software program and a username of

"datflypapi@Ares".

Additionally during this investigation, I also observed and successfully downloaded three (3) additional complete files from the computer with host IP address 65.96.142.191 on 03/09/2012 between 11:39:04 hrs and 11:55:06 hrs (EST). I reviewed the files that were downloaded and based on my training and experience I believe these files to be child pornography in violation of MGL Chapter 272 §§ 29B and 29C. The downloaded files are described below:

- a) *Original filename: Information about the filename not supplied by remote host computer.*

SHA-1: 5BMS5RQHQZXW3ZPHW50J3334GM2V6CAI

Description: This file is a webcam type video that is approximately seven minutes and fifty-three seconds in length depicting two young prepubescent females that appear approximately 8 to 10 years old in various stages of nudity. One of the females sticks her nude buttocks into the camera's view exposing her anus and vagina. Both females are then observed fully nude posing for the camera with exposed breasts and vaginas. Both female's then spread their legs wide exposing their vaginas and then have close up shots of their vaginas with the camera. The female's are then seen masturbating their vaginas. One of the female's inserts her finger into her anus at one point of the video.

- b) *Original filename: !!new pthc dark studio 10yro spread wide(2).avi*

SHA-1: Z5KUC5K2DADD77BZMQENMV3LB2WDVGKT

Description: This file is a video that is approximately five minutes and twenty-eight seconds in length depicting a young nude prepubescent female that appears approximately 10 to 12 years old leaning back on a couch. Her breasts are exposed and she is masturbating her vagina with her hand. She is observed inserting her finger into her vagina while licking her lips. At other various points in the video she is spreading her legs and vagina with her hands. She is then observed urinating into a toilet.

- c) *Original filename: stickam sisters(2).avi*

SHA-1: 63460CD5FR7YSVSSLRPSPCIETA5TDFA

Description: This file is a webcam type video that is approximately one hour four minutes and nine seconds in length depicting two young prepubescent females that appear approximately 10 to 12 years old posing for the camera in various stages of nudity. One of the females sticks her nude pelvic area into the camera's view exposing her vagina.

On the same date and time that the downloads from the remote host computer occurred, I observed the remote host computer's IP Address 65.96.142.191 in the Ares client used in this investigation. I further caused a NETSTAT³ command to be executed.

³ Netstat is a program which causes the connections to a computer at the time the program is run to be displayed. Depending upon the parameters given to the program, the output may show the IP address of the connection in numerical

several times during the download process in an effort to further verify the sharing host's IP Address and that I was directly connected to the remote host computer with IP Address 65.96.142.191 during the download process. I reviewed the logs created by using the NETSTAT command. These logs showed that on 03/09/2012 between 11:31:12 hrs (EST) and 12:01:24 hrs (EST) a computer with the Host IP address 65.96.142.191 was periodically connected to the computer upon which I was conducting the investigation.

I conducted an Internet search on the origin of the IP address 65.96.142.191 and found it to be issued to the internet service provider, Comcast Cable. As a result of this information, the Berkshire County District Attorney's Office issued an Administrative Subpoena to require Comcast Cable to provide records and other information pertaining to its respective subscriber on 03/09/2012 between 11:31:12 hrs (EST) and 12:01:24 hrs (EST) for IP Address 65.96.142.191.

On 03/15/2012, Comcast Cable responded to said Order indicating that the following subscriber had been assigned the IP address 65.96.142.191 on 03/09/2012 between 11:31:12 hrs (EST) and 12:01:24 hrs (EST):

| | |
|------------------|--|
| Subscriber Name: | Angel Martinez |
| Service Address: | 231 Sunset HL Fall River, MA 02724-3753 |
| Telephone #: | 774-253-9719 |

Based upon the above initial investigation, I am referring this investigation and all evidence generated during the investigation to Detective Steven Washington of the Fall River Police Major Crimes Division.

Sergeant Michael Hill

Massachusetts State Police
Massachusetts Internet Crimes Against Children Task Force Commander

7. On 03/22/12 I, Det. Steven Washington was assigned to continue Sgt. Michael Hill's investigation.

8. I have viewed the files that were downloaded by Sgt. Michael Hill and agree with the

or named form. When the "netstat" command is executed during a file transfer between computers, the output will include the IP address or name of the computer(s) which transferred the file(s).

Search Warrant Affidavit for 231 Sunset Hill in Fall River Massachusetts

Page: 5 of 8

R.A./15

SW 4/3/12 4/3/12 JEF

descriptions of those files by him. Based upon my training and experience, each of the digital files appear to be Child Pornography in violation of Chapter 272 Section 29B and 29C of the Massachusetts General Laws.

9. On 04/02/11 at approximately 1100 hrs I went to 231 Sunset Hill and observed it to be a part of the Sunset Hill Housing Development.

10. I verified that 231 Sunset Hill is occupied by Maria Avilez 08/17/45, who is the Mother of Angel Martinez 03/27/83.

11. I know from training and experience that those who have possessed and/or disseminated child pornography have an interest or preference in the sexual activity of children. Those who have demonstrated an interest or preference in sexual activity with children or in sexually explicit visual images depicting children are likely to keep secreted, but readily at hand, sexually explicit visual images depicting children. In some instances, these depictions are actual photographs or images of the suspect's own sexual activity with past or present children. In some instances, the suspect keeps these depictions as a means of plying, broaching, or titillating the sexual interests of new child victims or otherwise lowering the inhibitions of other potential child sexual partners by showing them that other children participate in this kind of activity. Still, in other instances, the depictions are a means of arousing the suspect. These depictions tend to be extremely important to such individuals and are likely to remain in the possession of or under the control of such an individual for extensive time periods. Although he might, a person who has this type of material is not likely to destroy the collection. These sexually explicit visual images depicting children can be in the form of, but not limited to, negatives, slides, books, magazines, videotapes, photographs or other similar visual reproduction, or by an image/video depiction by computer.

12. I know from training and experience that persons trading in, receiving, distributing or possessing of images or movies involving child pornography will make copies of those files on their computer's hard drive or other removable media. These computer storage media devices can be and have been found within the person's residence, on the person, and within their motor vehicles.

13. I know from my training and experience that even if a user deleted the files, they still may be recoverable by a trained computer forensic examiner.

14. I know from training and experience that persons trading in, receiving, distributing or possessing images or movies involving the exploitation of children or those interested in the actual exploitation of children often communicate with others through correspondence or other documents (whether digital or written) which could tend to identify the origin of the images as well as provide evidence of a persons interest in child pornography or child exploitation.

15. I know from training and experience that individuals who have a sexual interest in children and have access to the Internet will conduct searches for child pornography and

child sex stories on the Internet using Internet search engines or other programs that share files via the Internet. These individuals will use terms that are associated with children, nudity, and sex. These searches can be found within Internet history files, such as Internet Explorer History, or within unallocated areas of the hard drive.

16. I know from training and experience that files related to the exploitation of children found on computers are usually obtained from the Internet using application software which often leaves files, logs, or file remnants which would tend to show the exchange, transfer, distribution, possession, or origin of the files.

17. I know from training and experience that computers used to access the Internet usually contain files, logs, or file remnants, which would tend to show ownership and use of the computer as well as ownership and use of Internet service accounts used for the Internet access.

18. I know from training and experience that search warrants of residences involved in computer related criminal activity usually produces items that would tend to establish ownership or use of computers and ownership or use of any Internet service accounts accessed to obtain child pornography to include credit card bills, telephone bills, correspondence, and other identification documents.

19. I know from training and experience that search warrants of residences usually reveals items that would tend to show dominion and control of the property searched, to include utility bills, telephone bills, correspondence, rental agreements, and other identification documents.

20. I also have knowledge, based upon my experience and training that if untrained persons are allowed into a crime scene, they may unintentionally disturb, damage, or obliterate crucial evidence. Accordingly, while the crime scene search warrant is being executed, I respectfully seek the court's authority to impound and secure the premises and to keep out all unauthorized persons not assigned to the investigation.

21. Based upon the above, there is probable cause to believe that a computer or computers located at the property of 231 Sunset Hill, has installed an Ares peer to peer file sharing software client. There is also probable cause to believe that this software has been used to download and offer for distribution child pornography in violation of Massachusetts General Law Chapter 272 §§ 29 (governing obscene matter crimes), 29B (governing the crime of the possession with intent to disseminate child pornography), and 29C (governing the crime of the possession of child pornography).

22. There is probable cause to believe that the items annexed in Appendix A (attached) are evidence of the attempted exploitation of children in violation of Massachusetts General Law Chapter 272 §§ 29 (governing obscene matter crimes), 29B (governing the crime of the possession with intent to disseminate child pornography), and 29C (governing the crime of the possession of child pornography).

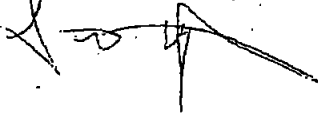
(attached) are evidence of the attempted exploitation of children in violation of Massachusetts General Law Chapter 272 §§ 29 (governing obscene matter crimes), 29B (governing the crime of the possession with intent to disseminate child pornography), and 29C (governing the crime of the possession of child pornography).

23. I respectfully request that the Court issue a warrant and order of seizure, authorizing the search of the property located at 231 Sunset Hill in Fall River Massachusetts, described previously in above Paragraph #13, and search for those items listed in "Appendix A" (And with regard to such "computer systems" to transport the same to a secure location anywhere in the Commonwealth of Massachusetts and, there, to SEARCH therein for and SEIZE). Said "Appendix A" will be attached to the face of the warrant.

Signed under the pains and penalties of perjury this April 3rd, 2012.

Before

Det. Steven Washington



Clerk Magistrate

Peer to Peer File Sharing

Based on my training and experience, I know the following regarding Peer to Peer file sharing networks, Peer to Peer client software programs, and the Ares Peer to Peer file sharing network.

A growing phenomenon on the Internet is peer to peer (hereinafter referred to as "P2P") file sharing. P2P file sharing is a method of communication available to Internet users through the use of special software programs. P2P file sharing programs allow groups of computers using the same file sharing network and protocols to transfer digital files from one computer system to another while connected to a network, usually on the Internet. There are multiple types of P2P file sharing networks on the Internet. To connect to a particular P2P file sharing network, a user first obtains a P2P client software program for a particular P2P file sharing network, which can be downloaded from the Internet. A particular P2P file sharing network may have many different P2P client software programs that allow access to that particular P2P file sharing network. Additionally, a particular P2P client software program may be able to access multiple P2P file sharing networks. These P2P client software programs share common protocols for network access and file sharing. The user interface, features, and configurations may vary between clients and versions of the same client.

In general, P2P client software allows the user to set up file(s) on a computer to be shared on a P2P file sharing network with other users running compatible P2P client software. A user can also obtain files by opening the P2P client software on the user's computer and conducting a search for files that are of interest and currently being shared on a P2P file sharing network.

Some P2P file sharing networks are designed to allow users to download files and frequently provide enhanced capabilities to reward the sharing of files by providing reduced wait periods, higher user ratings, or other benefits. In some instances, users are not allowed to download files if they are not sharing files. Typically, settings within these programs control sharing thresholds.

Typically, during a default installation of a P2P client software program, settings are established which configure the host computer to share files. Depending upon the P2P client

software used, a user may have the ability to reconfigure some of those settings during installation or after the installation has been completed.

Typically, a setting establishes the location of one or more directories or folders whose contents (digital files) are made available for distribution to other P2P clients. In some clients, individual files can also be shared.

Typically, a setting controls whether or not files are made available for distribution to other P2P clients.

Typically, a setting controls whether or not users will be able to share portions of a file while they are in the process of downloading the entire file. This feature increases the efficiency of the network by putting more copies of file segments on the network for distribution.

Files being shared by P2P clients are processed by the client software. As part of this processing, a hashed algorithm value is computed for each file being shared, which uniquely identifies it on the network. A file processed by this hash algorithm operation results in the creation of an associated hash value often referred to as a digital signature. Some hash algorithms provide a certainty exceeding 99.99 percent that two or more files with the same hash value are identical copies of the same file regardless of their file names. By using a hash algorithm to uniquely identify files on a P2P network, it improves the network efficiency. Because of this, typically, users may receive a selected file from numerous sources by accepting segments of the same file from multiple clients and then reassembling the complete file on the local computer. This is referred to as multiple source downloads. The client program succeeds in reassembling the file from different sources only if all the segments came from exact copies of the same file. P2P file sharing networks use hash values to ensure exact copies of the same file are used during this process.

P2P file sharing networks, including the Ares network, are frequently used to trade digital files of child pornography. These files include both image and movie files.

The Ares network is an open source public file-sharing network. Most computers that are part of this network are referred to as "nodes". The terms "nodes" and "clients" can be used interchangeably when referring to the Ares network. A node can simultaneously provide files to some nodes while downloading files from other nodes. Nodes may be elevated to temporary indexing servers referred to as "supernodes". Supernodes increase the efficiency of the Ares

network by maintaining an index of the contents of network nodes. Ares users query supernodes for files and are directed to one or more nodes sharing that file. There are many supernodes on the network, if one shuts down the network continues to operate.

The Ares network can be accessed by computers running many different client programs, some of which include the original Ares Galaxy client program, and derivatives compiled from the source code which is open source and freely available. These programs share common protocols for network access and file sharing. The user interface, features, and configuration may vary between clients and versions of the same client. Ares Galaxy is a free P2P client software program that can be downloaded from the Internet.

During the installation of an Ares client, various settings are established which configure the host computer to share files. Depending upon the Ares client used, a user may have the ability to reconfigure some of those settings during installation or after the installation has been completed. Typically, a setting establishes the location of one or more directories or folders whose contents (files) are made available to other Ares users to download. This location is commonly referred to as the "My Shared Folder" and in many versions is defaulted to be on the computer's "Desktop".

The Ares client software processes files located in a user's shared directory. As part of this processing, a SHA-1¹ hash value is computed by the client software for each file in the user's shared directory.

The Ares network uses SHA-1 hash values to improve network efficiency. Users may receive a selected file from numerous sources by accepting segments of the file from multiple users and then reassembling the complete file on the local computer. The client program succeeds in reassembling the file from different sources only if all the segments came from exact copies of the same file. The Ares network uses SHA-1 hash values to ensure exact copies of the same file are used during this process.

¹ SHA1 or Secure Hash Algorithm Version 1 is a file encryption method which may be used to produce a unique digital signature of a file. Finding a file that produces the same SHA-1 value as a known file requires a search and comparison of 10^{28} (2^{160}) different files, which is computationally infeasible. The Secure Hash Algorithm (SHA) was developed by the National Institute of Standards and Technology (NIST), along with the National Security Agency (NSA), for use with the Digital Signature Standard (DSS) as specified within the Secure Hash Standard (SHS). The United States of America has adopted the SHA-1 hash algorithm described herein as a Federal Information Processing Standard.

Typically, when a user launches the Ares client program, the client program will likely connect to one or more supernode(s) on the Ares network. Once connected to a supernode(s), information about the files the user is sharing is provided to that supernode(s). Such information may include a list of the files being shared and other descriptive information about those files, including the files' SHA-1 hash value(s). This allows other users on the Ares network to locate these files. The frequency of updating this information is dependent upon the client software being used and the Ares networking protocols. This information sent to the supernode(s) is data about the file and not the actual file itself. The file remains on the remote user's computer. In this capacity, the supernode(s) acts as a pointer to the files located on a remote user's computer.

The Ares network supernode(s) assists the Ares client users in locating files based on the keyword terms searched for by the user. When a user wants to find a file on the Ares network, the user enters a keyword search into the Ares client search screen menu. This initiates a keyword search request to the supernode(s). The supernode(s) will return a list of file names (not the files themselves) that match the search criteria. This information comes from nodes that have recently reported to a supernode(s) that they (nodes) had a file(s) with the keyword search term in the file name(s). Each file name returned is mapped to a SHA-1 hash value, which uniquely identifies the file on the Ares network. In order for the user to obtain the actual file, the user must manually initiate a download process, typically by double clicking on the file name. The user can identify the file(s) they wish download by the file name. When the download process of the file actually begins, the download of the file occurs from one or more nodes (not the supernode[s]).

Once a user initiates the download of a particular file, the user is presented with a list of users (nodes) who had recently broadcast to the Ares network that they have the requested file available for others to download. Typically, the supernode(s) on the network return this list containing the remote node information and the Internet Protocol (IP) addresses² of computers which have recently reported they have the same file (based on SHA-1 hash value comparison),

² Computers on the Internet identify each other by an Internet Protocol or IP address. IP addresses can assist law enforcement in finding a particular computer on the Internet. IP addresses can typically lead the law enforcement officer to a particular Internet service company and that company can typically identify the account that used the IP address to access the Internet.

or in some instances, portions of the same file available to others to download. Typically, once the Ares client has downloaded part of a file, it may immediately begin sharing the file with other users.

Obtaining files from the Ares network, as described herein, returns the candidate list, including IP addresses, which can be used to identify the location of computers. Although the IP address is not usually visible to the end user in the common Ares clients, it is returned and used by the software to initiate the download.

Law Enforcement has modified an Ares client program to allow the downloading of a file from a single IP address as well as displaying the IP address and SHA-1 hash value, which is known to all Ares clients but not typically displayed to the end user. This procedure allows for the detection and investigation of those computers involved in sharing digital files of known actual child pornography.

Typically, as described above, one method for an investigator to search the Ares network for users possessing and/or disseminating child pornography files is to type in search terms, based on their training and experience, that would return file name results indicative of child pornography. The investigator would then download the file and determine if it indeed contained child pornography. If so, the investigator can document the SHA-1 hash value of this file, to be compared with future identical files observed on the Ares network. Although transparent to the typical user, when searches are conducted, additional results are received from the Ares supernode(s) or other nodes, which may include the SHA-1 hash value of the file and the IP addresses of clients who recently reported to the network as having that file in whole or in part. This information can be documented by investigators and compared to those SHA-1 hash values the investigator has obtained in the past and believes to be child pornography. This allows for the detection and investigation of computers involved in possessing, receiving, and/or distributing files of previously identified child pornography. Therefore, without even downloading the file, the investigator can compare the SHA-1 hash value and determine with mathematical certainty that a file seen on the network is an identical copy of a child pornography file they had seen before.

The returned list of IP addresses can include computers that are likely to be within the investigator's jurisdiction. The ability to identify the approximate location of these IP addresses is provided by IP geographic mapping services, which are publicly available and also used for marketing and fraud detection. At this point in the investigative process, an association between a known file (based upon on the SHA-1 hash value comparison) and a computer having a specific IP address (likely to be located within a specific region) can be established.

Once a client user is identified as recently having a file believed to be child pornography, in whole or in part, the investigator can then query that client user directly to confirm the client user has that file, in whole or in part, and/or download that file directly from the client user exclusively, otherwise known as a single source download. Depending upon several factors, including configuration and available resources, it might not be possible to do either. The process of sharing files on the Ares network involves nodes allowing other nodes to copy a file or portions of a file. This sharing process does not remove the file from the computer sharing the file. This process places a copy of the file on the computer which downloaded it.

If an investigator either received an affirmative response from a remote node that they possess a digital file, or the investigator received a digital file, in whole or in part, that is believed to contain child pornography, from a remote node at a specific IP address, the investigator can conclude that a computer, likely to be in this jurisdiction, is running an Ares P2P client and is currently possessing, receiving, and/or distributing specific and known visual depictions of child pornography.

During the query and/or downloading process from a remote Ares client, certain information is exchanged between the investigator's client and the remote client they are querying and/or downloading a file from. Such as 1) the remote client's IP address; 2) a confirmation from the remote client that they have the file(s) being requested, in whole or in part, and that the file(s) is being reported as shared from the remote client program; 3) the file's corresponding SHA-1 hash value(s); 4) the remote client's "username"; and 5) the remote client program and version. Typically, the Ares program on installation prompts the user to enter a nickname for use in peer to peer chat features the software may have, which would be equivalent to a client's "username". This information may remain on the remote client's computer system

for long periods of time. The investigator has the ability to log this information. A search can later be conducted on a seized computer system(s) for this information, which may provide further evidence that the investigator's client communicated with the remote client.

An analogy to this investigative methodology would be receiving information from an informant or an anonymous source that a particular residence was selling illegal narcotics. An undercover investigator could independently confirm this information by knocking on the door of the residence and asking if they had said illegal narcotics. If so, the undercover investigator would then ask for and receive the said illegal narcotics without actually entering the residence, which would be similar to asking for and receiving an illegal child pornography file from a P2P client.

The investigation of peer-to-peer file sharing networks is a cooperative effort of law enforcement agencies around the country. Many of these agencies are associated with the Internet Crimes against Children Task Force Program. P2P investigative methodology has led to the issuance and execution of search warrants around the country resulting in the arrest and conviction of numerous offenders possessing and/or distributing child pornography, some of which were also involved in the sexual exploitation of actual child victims.

Exhibit 2

Information Related to the Seizure and Searching of Digital Evidence

1. This addendum seeks to explain what a search for computer related items may involve, the subsequent search of the computer storage devices seized; and further justify the following as a necessary part of the search process:

- I. The seizure of all computer hardware and software and any operating manuals from the authorized location.
- II. The searching of all areas of the authorized location for computer related evidence.
- III. The photographing of the authorized location including the computer systems.
- IV. The removal of the computer system, and related computer peripherals, software and storage media to an off-site controlled environment to perform the search and analysis of the data for the specific authorized items.

2. Computers can exist either as a "stand alone" computer or as part of a bigger computer network, a "networked computer". A "stand alone" computer is one that is isolated from or not attached to any other computer. A "stand alone" computer is becoming rarer into today's high tech interconnected world. A "networked computer" is one that is connected to, attached to or can communicate with other computers or hosts. "Network computers" can share computer services with other computers such as file sharing, file storage, remote administration, email, printing and many more. For example, a computer in a home may have a printer attached to it. Other computers on the home network can print to that printer because the host computer is sharing that resource. Most computers today have the ability to become networked, even temporarily, when they attach to the internet through a dial up modem.

3. A stand alone "computer system" is sometimes referred to as a work station, personal computer or laptop and generally is composed of two parts; hardware and software. The hardware components can generally be broken down into four common categories; system components, storage devices, input and output devices. The software can be broken down into two categories; operating systems and application software. Software are the tools that allow a user to produce data files which are ultimately stored on the computer's data storage devices.

4. The system components are generally installed inside a case or chassis. They include but are not limited to the system board, central processing unit (CPU), random access

Exhibit 2

Information Related to the Seizure and Searching of Digital Evidence

memory (RAM), read only memory (ROM), cache memory, add on boards and a power supply. The most important computer system component is the system board, commonly referred to as the "motherboard". It is an electronic circuit board that all other circuit boards or other electronic devices plug into. The "CPU" or central processing unit is the brain of the computer. Its function is to organize the requested actions received from the components. The processor receives requests, determines what tasks the computer needs to perform to fulfill those requests, and translates those tasks into electronic signals the required devices can understand. The processor does the math and logical calculations. The processor is plugged into the motherboard.

5. Memory can take various forms including RAM, ROM and Cache. The most common is Random Access Memory or RAM. RAM is used to temporarily store instructions and data that the CPU will need. The information in RAM is very volatile and is constantly being read, written, changed and removed. When power to the computer is lost all the information in RAM is lost as well. ROM is read only memory. ROM is usually a computer chip installed on the mother board that has computer instructions or data permanently imprinted on it. Cache memory is usually a memory chip installed on the CPU or very close to the CPU. It is usually much faster for the CPU to read the Cache memory than it is to read the Random Access Memory. Because memory is volatile and information will be lost when the computer loses power, information that is evidentiary in nature that is in memory will be lost as well. Therefore, it may be necessary for the investigator to perform some processing to secure the information in RAM prior to the computer being powered down. An example would be a word processing document that has not yet been saved or the current state of the computer's network connections.

6. Probably the most important component of a computer system, to a criminal investigator, are the computer's storage devices. Storage devices is a technology that is changing at an extremely fast pace both in terms of the type of storage devices available and the quantity of data the storage device is capable of holding. The storage device holds or stores information or data, even when the computer's power is turned off. The data stored on the storage devices are kept unless they are manually removed or altered by the user or the computer's software.

Often computer systems have multiple storage devices. Traditionally these storage devices were hard drives that were installed inside of a computer case. They were

Exhibit 2

Information Related to the Seizure and Searching of Digital Evidence

attached to the computer's mother board by cables referred to as ribbon cable and were powered from the computer's internal power supply. Today, internally installed hard drives are still a major component of a computer system, however, the availability and popularity of external hard drive storage devices or enclosures is growing rapidly. These external hard drive devices have become more readily available to the consumer over the past few years. New technologies such as USB, Fire wire and wireless connectivity allow data transfer rates between the computer and the hard drive at speeds that were not possible prior. These hard drives work the same way as the internal hard drives, what makes them different is that they are external to the computer and therefore removable and portable. These removable hard drive storage devices allow a user to plug the device into a computer system, read from or write to the device and then unplug the device and store it somewhere away from the computer. It could be used to move files from one computer to another. A user could plug the device into a computer at work, copy files to the removable storage media, bring the device home, attached to the home computer and copy the files to the home computers hard drives. These devices therefore could be located almost anywhere within a home or business that is the subject of a search.

7. Removable storage is the other area that is changing at rapid pace and the criminal investigator needs to consider just how portable and small removable storage devices can be. Removable storage traditionally consisted of floppy diskettes. Floppy diskettes are still popular today. They are small removable storage devices that are placed inside of a floppy diskette drive. The amount of storage space is somewhat limited and is normally 1.44 megabytes on a 3.5 inch floppy diskette drive. The need for greater removable storage has lead to the development of different technologies. One of these technologies is compact disc or CD. Compact discs are storage devices that are capable of storing computer files and can generally store 650 MB of data. This is approximately 450 times more data than floppy diskettes. Compact Discs originally could only be read from and not written to. However, compacts discs have changed and now can be both read from and written to multiple times much like a floppy diskette. Other portable storage solutions exist including USB portable storage devices, sometimes referred to as "flash drives" or "thumb drives". These are very small devices that can fit into a person's pocket. They plug into the computer's USB port and allow a user to store up to sixty gigabytes of data. These devices today are being manufactured to look like they are not computer storage

Exhibit 2

Information Related to the Seizure and Searching of Digital Evidence

devices at all. This includes USB storage devices that are built into writing pens and wrist watches. Other types of removable or external storage devices are tapes and tape drives, zip drives and zip disks, digital video disk drives and digital video discs (DVD) and flash media. These removable media are portable and have the ability to store large amounts of data. They can be easily concealed and carried off in a shirt pocket, on a key chain, or in a wallet.

8. Other digital devices such as personal digital assistants (PDA), cellular telephones, MP3 players, tablet computer devices (such as iPads, Nooks, etc...) all have the ability to store data and be connected to a computer and data transferred to or from the device and the computer. The presence of these storage devices needs to be considered during the search for digital evidence. Again, these devices can be very small and easily hidden. Although an MP3 player is made to store and play back MP3 audio files, usually music; it is a digital device and any type of file could be stored on it, including image and video files. The newest cellular telephones have the ability to access the internet, email, send and/or receive photo's and have an extensive address book.

9. Computer input and output devices are commonly referred to as "computer peripherals" or "peripheral devices". They tend to be external devices (outside the computer's case) although connected in some manner to the computer system. Input devices are devices that allow a user to input data or instructions into the computer system for processing. They commonly include keyboards, mice, scanners, digital cameras and microphones. Other less common "input devices" may also be present as part of a computer system, but usually to accomplish a specialized function. These devices can be connected to the computer using a wired or wireless technology.

10. Output devices are components through which the computer sends or "outputs" data. The monitor is a visual device that displays the primary output of a computer. The printer is another important output device. It produces output in the form of paper often referred to as hard copy. Printers take a variety of forms including ink jet, laser and dot matrix printers. Computer speakers are an example of an output device that outputs the audio sound from the computer. Other less common "output devices" may be present as part of a computer system usually to accomplish a specialized function. These devices can be connected to the computer using a wired or wireless technology.

Exhibit 2

Information Related to the Seizure and Searching of Digital Evidence

11. The second category of a typical "computer system" is "software". Software typically is categorized into two general sub-categories: operating system software and application software. In some instances, it is hard to make a distinction whether some program is part of the operating system or a separate application.

12. "Operating Systems" are software programs designed to instruct the computer how to "operate". These instructions control how the system will process data, run applications and which hardware will function. There are many different operating systems. Common operating systems include products made by Microsoft Corporation including Windows 95, 98, ME, 2000, XP Home, XP Professional, and Vista. There are hundreds of operating systems and variants including but not limited to DOS, Linux, FreeBSD, Macintosh and UNIX. As operating systems mature they offer additional features. Many of the newer operating systems implement features that focus on security and privacy. As an example, an operating system can be configured to require a user name and password to gain access to the computer. Some operating systems have logs that keep track of various events on the computer. An example may be a log that keeps track of both successful authorized logins, as well as attempted logins that failed. In addition, operating systems may implement methods of storing data in more secure compressed, password protected or encrypted formats. When compression, password protection, and encryption are used, it makes keyword searches ineffective without first uncompressing or decrypting the files containing the data. Computers installed in a home environment are less likely to have implemented security procedures than are computers in a business environment.

13. "Applications" are computer programs designed to be used by a user to perform some function or service for the user. Application software makes requests of the operating system to perform various tasks. There are many different types of application software. Common applications include programs such as spreadsheet, word processing, database, graphic design, accounting, web browsing, and e-mail. Other software applications are designed to protect, hide, securely delete, encrypt, compress or password protect data. It is important to remember that software almost always has a legitimate purpose and security and privacy of a user's data is a legitimate purpose; however, a person can also use this software to conceal, delete or disguise records of illegal activities. Software applications, don't necessarily store the information in a human readable format on the hard drive. They store the information in a

Exhibit 2

Information Related to the Seizure and Searching of Digital Evidence

format that the program understands and the program, when asked, presents that data on an output device in a human readable format.

14. Networked computers are one or more stand alone computers that have the ability to communicate with each other. In order to communicate with another computer, a computer must have some physical device to allow the communication to occur. These devices include but are not limited to modems, network cards or wireless network cards. Today more and more people have small networks in their homes. This may be two or more computers connected together to share a printer or internet connection.

15. A modem is a physical device that may either be installed within or attached to a computer system. A modem allows a computer to call another computer that also has a modem using traditional telephone lines. A network card is a physical device installed either inside or external to the computer and allows the computer to be connected to another computer via a wire or cable of some type. An example would be in a business environment where a user's workstation is attached to a server. Commonly found in homes today are both cable modems and digital service line ("DSL") modems. These allow users to have much faster connections to the internet than was provided by a dial up telephone connection. The internet service provider in these cases are a cable TV company or a telephone company. In addition, these types of connections are "always on". Since there is no dialing involved a user is always connected.

16. A wireless network card allows a computer to communicate to another computer via the radio spectrum; much like a cordless telephone allows a user to move around their house with a telephone.

17. A computer can offer services to a requesting computer. One of the services offered may be data storage services. This allows a user to store or retrieve data from or to a computer that could be hundreds or thousands of miles away. The user in today's world no longer needs a file or program to be stored locally (on its own hard drive); they can run the program, write or retrieve a file that is many miles away, even in a foreign country. Network storage services are prevalent on the internet today.

18. A computer system is an integrated system, it is necessary to have all the elements of that system in order to accurately retrieve and preserve evidence contained on that system. It is sometimes difficult, if not impossible, if you do not have the original hardware. As an

Exhibit 2

Information Related to the Seizure and Searching of Digital Evidence

example, one of the processes used by computer forensic personnel is to make an exact copy of the subject hard drive on to another drive. This copy could with some older operating systems be placed inside of a different computer and it would start up fine; however, with today's operating systems there are hardware and software conflicts that prevent this copied drive from operating correctly inside of a foreign computer and the forensic examiner is forced to place the copy back in the original computer in order to boot or start the computer. As another example, a file may have been created with a particular version of software, in a particular format, capable of only being reasonably outputted on a printer on that system. Because of the multiplicity of computer systems available and the almost limitless number of operating system and application software, attempting to retrieve and preserve evidence from a computer system without the computer on which it was generated or saved, it will not only be unreasonably time consuming, but costly as well. For these reasons, it is more reasonable to seize the entire computer system, all storage media, input and output devices, all software, and any documentation associated with that software. To do this work accurately and completely requires the seizure of all computer equipment and peripherals, which, may be interdependent, the software to operate the computer system, and the instructions manuals for the computer system and software programs.

19. In addition, the search for computer storage devices and media needs to be extensive to be complete. As mentioned, the computer system itself is but one piece of the evidence. Storage media is small and can be easily hidden. Therefore a thorough search of the premises that is the subject to the search must be made, including all persons present.

20. The seizure of software manuals is necessary because of the vast quantity of software on the market. The forensic examiner can not possibly know each and every type of software available and the manuals may provide needed information. Computer users are also known to write down user names, passwords or access codes or other important information needed to gain access to the computer, to execute a program or to open a file, on paper or record them in some manner. It is necessary for the criminal investigator to search for items of this nature.

21. The physical set up of the computer can be complicated with cables connecting different devices. It is necessary that the investigator accurately and completely document the state of the computer system. This documentation should include photographing all aspects of

Exhibit 2

Information Related to the Seizure and Searching of Digital Evidence

the computer system including, but not limited to, what is visible on the monitor at the time of the search, the cabling, the peripherals attached, and the overall physical location of the computer in the search location.

22. In most circumstances it is not reasonable to perform the search of computer media at the search site itself. In order to properly retrieve and analyze all electronically stored data, to document and authenticate such data, and to prevent the loss of the data from accidental or deliberate programmed destruction, it requires off-site laboratory analysis by a qualified computer specialist. Several factors justify the off-site search of the computer media including but not limited to; the quantity of the storage media, the storage capacity of that media, the physical environment of the search area, the nature of digital evidence in general, the nature of the crime under investigation, the nature of the evidence sought, the time involved to complete the search, the intrusion and the need to limit that intrusion or inconvenience to persons at the search site.

23. As already mentioned, the search for digital evidence may involve the seizure of multiple computers and a large quantity of removable media. The computer storage devices mentioned are capable of storing thousands of pages of information. A "byte" is the equivalent of storing a single letter typed at the keyboard. A kilobyte (KB) is one thousand bytes, a megabyte (MB) is one million bytes, a gigabyte (GB) is one thousand megabytes, and a terabyte is one thousand gigabytes. A 100 MB storage device would have the capacity of storing fifty thousand of pages of typewritten, double space text. Many computer systems that are purchase today contain a 200 GB hard drive or larger. These drives have the ability to store huge volumes of data. External hard disk drives are now being sold having a one terabyte capacity.

24. The size of a storage device is but one issue when it comes to locating a file or files that are the target of a search. The software used to create or store the file may be such that it is not conducive to finding it with keyword searching. As mentioned, software may save data in a proprietary format, in an encrypted or compressed format that is not human readable and therefore not conducive to key word searching. In addition, the user can take other steps that inhibit law enforcement from discovering the information that is the subject of the search. This includes but is not limited to renaming files or file extensions, using encryption or compression, password protecting files or using software specifically designed to allow a user to hide the

Exhibit 2

Information Related to the Seizure and Searching of Digital Evidence

geometry of a drive, or to embed a file within another file or files. A user does not need extensive computer knowledge to perform these steps and software is readily available for free on the internet that will perform these steps for the user.

25. Most searches are performed in physical environments that are not favorable to proper methods of searching computers. The location itself may be limited in size. Computers require electrical power and many locations lack proper lighting and the availability of power. Search locations tend to be hostile in nature. The equipment brought to a scene to perform a search is expensive and can easily be broken. The controlled environment needed to perform an electronic search is most times not present.

26. The nature of digital evidence in general effects the ability to perform a search onsite. Digital evidence is extremely sensitive and can be altered or destroyed by both intentional as well as unintentional acts. Software programs installed on the subject's computer can perform actions that are unanticipated or can be set to run at various dates and times that would alter or change the state of the computer and its storage devices. Computer evidence is extremely vulnerable to tampering or destruction, both from external sources and from destructive codes embedded in the system programs. It is necessary to perform searches in a more controlled environment. This includes the physical environment, as well as the hardware and software used to process the subject media.

27. A nature of the crime under investigation along with the type of evidence sought is important to consider. In a child pornography case, one of the important elements of that crime is knowledge of the nature and contents of the files. Simply finding child pornography on the storage media is not a thorough or complete enough search. Searching must be performed for evidence that can indicate how, when, and by whom a file was placed on the computer system. Who accessed the file, when was the file accessed and was the file sent to others? This type of information isn't clearly evident; the forensic examiner must review and analyze the various operating system and software configurations, the directory and folder structure, logs of computer activity, files created, modified or accessed around or about the time the file of evidentiary value was created, modified or accessed. From the information gathered, the forensic examiner must then draw reasonable conclusions concerning who had knowledge of the

Exhibit 2

Information Related to the Seizure and Searching of Digital Evidence

nature and contents of files and when. The searching for these files and the analysis of the information in these files can take a substantial amount of time.

28. This requires that personnel executing the search warrant must examine all the stored data to determine which particular files are relevant and fall within the scope of the warrant. This search process can take weeks or months, depending on the volume and complexity of the data stored, and it would be impractical to attempt this kind of data search onsite. The intrusion to the home or business required to perform this type of searching onsite would be far more intrusive than removing the items to a secure controlled location to perform the search.

29. The analysis of electronically stored data whether performed on-site or in a laboratory or other controlled environments, may entail any or all of several different techniques. Such techniques may include, but shall not be limited to, surveying various file folders or directories and the individual files they contain; opening or reading the first few pages of such files in order to determine their precise contents; scanning storage areas to discover and possibly recover deleted data, scanning storage areas for deliberately hidden files, performing electronic keyword searching through all electronic storage areas to determine whether these storage areas contain information related to the subject matter of the investigation and searching for associated files or data that would record information as to when the file was created, when it was last written to and when it was last accessed and by whom.

30. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. Search protocols are designed to protect the integrity of the evidence, and to recover hidden, erased, compressed, password protected or encrypted files.

31. A "file system" is a way of organizing directories and files on a storage device. Different operating systems keep track of where on the storage device they stored files using a "file system". Some of the common "file systems" are "FAT", "NTFS", "EXT3". The file system is a representation of the storage device's organization as opposed to the actual data that is stored inside of the files. In other words, the "file system" is like a table of contents or an index in a book; it is a mechanism that keeps track of where the actual file or data is on the hard drive. Each "File System" works in different ways. File systems have their own conventions for

Exhibit 2

Information Related to the Seizure and Searching of Digital Evidence

the naming of files, such as how long a name can be or what characters are permissible in a file name. In the DOS, Windows, OS/2, Macintosh, and Unix operating systems the file system is called hierarchical meaning that a file is placed inside of a folder or directory. The folder or directory may be located inside of another folder or directory. The path is the route from a logical starting location down through the sub directories to the file name. In Windows, a path is usually in the form of "driveletter:\directoryname\subdirectoryname\filename.extension". (C:\Windows\Desktop\Myfile.doc). When a file is deleted, it may still be possible to recover the file because the file system usually just changes the entry related to that file as to where a file is located, but does not actually go to the physical location on the storage media and remove the information at that physical location. Therefore it may be possible to recover deleted data for a substantial period of time after the deletion occurred.

32. For the purposes of this affidavit the terms "records", "documents", "materials" and "files" include all information preserved in any form – visual, magnetic, electronic or aural – including the originals and all non identical copies thereof, whether different from the original by reason of notations made on such copies or otherwise. These definitions apply regardless of the form in which such records, documents, materials, files may have been created or stored, including but not limited to any handmade form (such as writing, drawing, or painting, with any implement on a surface, directly or indirectly); photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies); mechanical form (such as writing, printing or typing); any electrical, electronic or magnetic form (such as tape recordings, cassettes, compact disks, or any information on electronic or magnetic storage device, such as floppy diskettes, hard disks, CD Rom discs, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Zip Drives, or electronic notebooks, as well as printouts or readouts from any magnetic storage device).

Exhibit 3

Biography of Sgt. Michael Hill

I, Michael J. Hill, am a Massachusetts State Police Officer and have been so since my graduation from the State Police Academy in New Braintree, Massachusetts, in October of 1993. From October of 1993, until July of 1995, I was assigned to the Uniform Branch of the Massachusetts State Police at the State Police Barracks Cheshire. Between July of 1995 and August of 2011, I was assigned to the Massachusetts State Police Division of Investigative Services as a member of the Berkshire County Detective Unit. This unit works in direct contact with the office of the Berkshire County District Attorney investigating major crimes in Berkshire County. In August of 2011, I was transferred to the Massachusetts State Police Digital Evidence & Multi-Media Section as the Massachusetts Internet Crimes Against Children Task Force Commander. During my career as a Massachusetts State Police Officer, I have received training from the Massachusetts State Police in criminal investigations. I have also received training from police officers who are trained and experienced in computer crime investigations. I have attended various computer crime investigation courses involving computer crime, seizure, and examination of computers. I am an Encase Certified Examiner. "Encase" is a computer forensic software program that is widely used and accepted by the law enforcement community to forensically examine computer media. I am also a Certified Forensic Computer Examiner (CFCE) with the International Association of Computer Investigative Specialists (IACIS). I have attended numerous trainings on crimes against children on the Internet, which includes crimes associated with child pornography. I am a member of the High Technology Crime Investigation Association (New England Chapter) and the Internet Crimes Against Children (ICAC) Task Force in Massachusetts. In the course of my police career, I have participated in numerous investigations involving murder, rape, sexual assault, child abuse, child pornography, computer related crimes, Internet related crimes, and other felony investigations. I have participated in numerous applications and executions of search warrants for these investigations. I have also conducted numerous forensic examinations of computer storage media. In March 2005, I attended a three day training related to the investigation of persons using Gnutella peer to peer (P2P) software on the Internet to collect and distribute child pornography. In April of 2008, I attended a one day training conducted by the Federal Bureau of Investigation related to the investigation of persons using Gnutella peer to peer (P2P) software on the Internet to collect and distribute child pornography. In April and May of 2011, I attended training related to the investigation of persons using the BitTorrent, eDonkey2000, and Kademlia peer to peer file sharing networks to collect and distribute child pornography. Additionally, I have worked with other investigators who have investigated those persons using the Ares P2P file sharing network to collect and distribute child pornography. Furthermore, I instruct law enforcement around the country on how to investigate the dissemination of child pornography via peer to peer file sharing networks.

I have attached a seven (7) page document detailing peer to peer file sharing networks, Peer to Peer client software programs, and the Ares Peer to Peer file sharing networks (See attached Exhibit #1).

Attachment "A"

Items to be Searched for

1. Any and all computer Systems, including, but not limited to:
 - a. System components, including, but not limited to: the computer chassis, motherboard, CPU, memory, add-on boards, cables, and power supplies;
 - b. Computer storage devices, removable storage devices and digital content, including, but not limited to:
 1. Floppy diskettes;
 2. Internal & external hard drives;
 3. Compact Discs, both read only & writeable (CD-ROM, CD-R, CD-RW);
 4. Digital Tapes;
 5. Zip/Jazz disks;
 6. VHS and VHS-like tapes;
 7. Digital Video Discs (DVD-ROM, DVD-R, DVD+R, DVD-RW, DVD+RW);
 8. PDAs (Personal Digital Assistants);
 9. MP3 Players;
 10. Digital Cameras;
 11. Cell Phones;
 12. Portable tablet computing devices; and
 13. Flash memory devices and/or flash memory cards.
 - c. Input devices, including, but not limited to:
 1. Keyboards, mice, trackballs, pointers, etc.;
 2. Scanners, digital cameras, video capture cards, microphones, modems, etc.;
 3. Floppy Diskette Drives, Digital Tape Drives, Writable Compact Disk Drives, Writable Digital Video Disk (DVD) Drives;
 4. Zip/Jazz drives;
 5. Video cassette recorders.
 - d. Output Devices, including, but not limited to:
 1. computer monitors;
 2. computer speakers;
 3. computer printers;
 4. Floppy Diskette Drives, Digital Tape Drives, Writable Compact Disk Drives, Writable Digital Video Disk (DVD) Drives;
 - e. Network Devices, including, but not limited to:
 1. Cable/DSL modems;
 2. Wired/Wireless Routers; and
 3. Network cards.
2. Computer System Documentation, including, but not limited to, Operating System and Application programming disks and Programming and Application manuals, books or brochures.

Attachment "A"

Items to be Searched for

3. Computer software, hardware, and related items to the sharing of Internet access over wired or wireless networks allowing multiple persons to appear on the Internet from the same IP address.
4. Items containing or displaying passwords, access codes, usernames, or other identifiers necessary to examine or access items, software, or information seized.
5. Any documents pertaining to the possession, receipt, origin, or distribution of images involving the exploitation of children.
6. Correspondence or other documents exhibiting an interest in the exploitation of children.
7. Items that would tend to establish ownership or use of computers and ownership or use of any Internet service accounts to include credit card bills, telephone bills, correspondence, and other identification documents.
8. Items that would tend to show ownership and control of the property searched, to include utility bills, telephone bills, correspondence, rental agreements, and other identification documents.
9. Photographing and/or videotaping of the residence to be searched.
10. Visually explicit images/videos, whether on paper or its equivalent, which includes but not limited to negatives, slides, books, magazines, videotapes, photographs or other similar visual reproduction, or depiction by computer (specifically including such images/videos as stored within computer storage devices as computer data files) depicting any child known or reasonably believed to be under the age of 18 years of age, in which the child is:
 - a. Actually or by simulation engaged in any act of sexual intercourse with any person or animal;
 - b. Actually or by simulation engaged in any act of sexual contact involving the sex organs of the child and the mouth, anus or sex organs of the child and the sex organs of another person or animal;
 - c. Actually or by simulation engaged in any act of masturbation;
 - d. Actually or by simulation portrayed as being the object of, or otherwise engaged in, any act of lewd fondling, touching, caressing involving another person or animal;
 - e. Actually or by simulation engaged in any act of excretion or urination within a sexual context;
 - f. Actually or by simulation portrayed or depicted as bound, fettered, or subject to sadistic, masochistic, or sadomasochistic abuse in any sexual context; or
 - g. Depicted or portrayed in any pose, posture or setting involving a lewd exhibition of the unclothed genitals, pubic area, buttocks or, if such person is female, a fully or partially developed breast of the child.
11. Authorizing officers to secure the above computer related items and transport them to an off-site secure location, to continue the search of the computer items and computer storage devices for the following items:
 - a. Computer files, data, or other similar visual reproduction containing any sexually explicit

Attachment "A"

Items to be Searched for

visual images/videos or depiction by computer, of any child whom the person knows or reasonably should know to be under the age of 18 years of age and such child is:

- i. Actually or by simulation engaged in any act of sexual intercourse with any person or animal;
 - ii. Actually or by simulation engaged in any act of sexual contact involving the sex organs of the child and the mouth, anus or sex organs of the child and the sex organs of another person or animal;
 - iii. Actually or by simulation engaged in any act of masturbation;
 - iv. Actually or by simulation portrayed as being the object of, or otherwise engaged in, any act of lewd fondling, touching, or caressing involving another person or animal;
 - v. Actually or by simulation engaged in any act of excretion or urination within a sexual context;
 - vi. Actually or by simulation portrayed or depicted as bound, fettered, or subject to sadistic, masochistic, or sadomasochistic abuse in any sexual context; or
 - vii. Depicted or portrayed in any pose, posture or setting involving a lewd exhibition of the unclothed genitals, pubic area, buttocks or, if such person is female, a fully or partially developed breast of the child.
- b. Computer data files, records, logs associated with any of the above described files which may identify, trace, or record the facts, including but not limited to the date, time, modification, alteration, transmission or receipt via the Internet or other networks of any of the computer files described above, including, but not limited to file menus, Internet browser history, cache directories, registry entries, logs, and files.
 - c. Computer data files in the form of email, instant messaging, chat logs, or other communication logs, the contents of which involves the attempt to find, possess, acquire, store, or distribute child pornography.
 - d. Internet searches, stored within a computer file or data, using Internet search engines or file sharing programs for child pornography.
 - e. Any and all files associated with the installation, configuration and use of any peer to peer file sharing client, such as Ares, Shareaza, Bearshare, Limewire, etc...
 - f. Computer files and/or data that assist in identifying use, custody, control, or ownership of the computer systems and the removable storage devices.
 - g. Computer files and/or data that contain passwords, access codes, usernames, or other identifiers necessary to examine or access items, software, or information seized.
 - h. Computer data files and/or data containing the following terms:
 - i. IP Address: 65.96.142.191.
 - ii. SHA1 value of: 5KNCHEMCKAXWXTG25Z2GQC4IQVBJ4CNJ
 - iii. File name of: webcam - vivi_moranginho04 (brasileirinha 7)(brasil pthc ptsc knabinoj menina garota).avi

Attachment "A"
Items to be Searched for

- iv. SHA1 value of **Z5KUC5K2DADD77BZMQENMV3LB2WDVGKT**
- v. File name of **!!new pthe dark studio 10yro spread wide(2).avi**
- vi. Ares Client Name: **datflypapi@Ares**

COMMONWEALTH OF MASSACHUSETTS

BRISTOL, ss.

DISTRICT COURT DEPARTMENT
FALL RIVER DIVISION
NO. 1232CR02700

COMMONWEALTH

v.

ADALBERTO MARTINEZ

MOTION TO SUPPRESS EVIDENCE

The defendant on the above-entitled matter moves, pursuant to Mass.R.Crim.P. 13, that this Honorable Court suppress from the use in evidence anything recovered as a result of a search and seizure made pursuant to Search Warrant number 9323 issued from Fall River District Court, including but not limited to, laptop computers. A copy of the warrant and affidavit are attached hereto.

The Defendant maintains that the issuance of a search warrant, the execution of the search warrant, the seizure of any items including any and all statements made by the Defendant, and the Defendant's arrest were illegal because:

- a. There was no probable cause to arrest the Defendant.
- b. The Affidavit in support of the Application for the Search warrant does not demonstrate probable cause on its face and is defective.
- c. The search warrant was improperly issued.
- d. The search preceded the arrest.
- e. There was no valid consent to search.
- f. There were no exigent circumstances which would authorize the warrantless search.
- g. The information in the affidavit is stale.

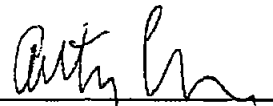
WHEREFORE, the Defendant maintains that his rights under the Fourth Amendment of the U.S. Constitution and Article Fourteen of the Declaration of Rights to the Constitution of the Commonwealth of Massachusetts have been violated.

After hearing, the court concludes that the Affidavit and accompanying exhibits in support of the Application for the search warrant for the premises at 231 Sunset Hill, Fall River, Ma. does provide probable

Adalberto Martinez,
By his attorney,

R.A./42

cause to believe contraband/evidence of specific criminal activity would be found there. The Defendant's motion is therefore DENIED. Summary 8-18-1



Anthony Clune
BBO # 663166
448 County Street
New Bedford, MA 02748
(508) 999-4088

Date: August 11, 2014

COMMONWEALTH OF MASSACHUSETTS

BRISTOL, ss.

DISTRICT COURT DEPARTMENT
FALL RIVER DIVISION
NO. 1232CR02700

COMMONWEALTH

v.


ADALBERTO MARTINEZ

AFFIDAVIT IN SUPPORT OF DEFENDANT'S MOTION TO SUPPRESS EVIDENCE

I, Anthony F. Clune, state the following is true to the best of my knowledge, information and belief:

1. I am an attorney duly licensed to practice law in this Commonwealth.
2. I am the attorney for the Defendant in the above matter.
3. I have heretofore been provided with a copy of the search warrant and the affidavit and application in support of the search warrant. I have read those documents and am familiar with the contents of same.
4. The affidavit does not indicate that the internet subscriber resided at the target address.
5. As a result of the execution of the search warrant, the police seized the items the Defendant seeks to suppress.
6. An examination of the affidavit in support of the application of the search warrant demonstrates that it is insufficient on its face to provide probable cause for the warrant to issue.
7. The Affidavit in Support of the Application for the Search Warrant does not set forth sufficient facts for a clerk magistrate to find probable cause that illegal contraband would be present upon the premises at the time the warrant was issued or executed.
8. I believe that the search warrant was defective and was improperly issued and executed.
9. There was no valid consent to search.
10. There were present no exigent circumstances, which would authorize a warrantless search.

Signed under the pains and penalties of perjury this 15th day of August, 2014.



Anthony Clune, Esq.

COMMONWEALTH OF MASSACHUSETTS

BRISTOL, ss.

DISTRICT COURT DEPARTMENT
FALL RIVER DIVISION
NO. 1232CR02700

COMMONWEALTH

v.

ADALBERTO MARTINEZ

MEMORANDUM OF LAW IN SUPPORT OF DEFENDANT'S MOTION TO
SUPPRESS EVIDENCE

Facts

1. On March 9, 2012, Sgt. Michael Hill of the Massachusetts State Police Internet Crimes Against Children Task Force was conducting investigations into the use of Peer to Peer(P2P) file sharing programs for the possession and distribution of child pornography.
2. Sgt. Hill observed a computer with an Internet Protocol (IP) Address of 65.96.142.191, which had child pornography files that it was sharing.
3. As a result of a subpoena, Comcast Cable indicated that the subscriber for IP Address, 65.96.142.191, was Angel Martinez, 231 Sunset HL, Fall River, MA 02724-3753, Telephone 774-253-9719.
4. On April 2, 2011, Det. Steven Washington went to 231 Sunset Hill and observed it to be part of the Sunset Hill Housing Development.
5. Det. Washington verified that 231 Sunset Hill was occupied by Maria Avilez who is the mother of Angel Martinez.

6. As a result, a warrant was issued for 231 Sunset Hill.

Argument

- I. THE FOUR CORNERS OF THE SEARCH WARRANT AFFIDAVIT CONTAINED INSUFFICIENT EVIDENCE TO PROVIDE PROBABLE CAUSE, RENDERING THE WARRANT INVALID.

The Supreme Judicial Court has held that G.L. c.276, Sec. 1A, and 2B require that warrants be issued only if there is a showing of probable cause, and that Sec. 2B requires the suppression of evidence seized pursuant to a warrant not based upon probable cause. *Commonwealth v. Upton*, 394 Mass. 363 (1985). The Court further stated that the word “cause” in Article 14 of the Declaration of Rights of the Constitution of the Commonwealth is used synonymously with “probable cause” *Id.* In *Upton*, the Supreme Judicial Court concluded that Article 14 provides more substantive protection to criminal defendants than does the Fourth Amendment in the determination of probable cause. *Id.* The “totality of the circumstances” test by the United States Supreme Court was expressly rejected by the Supreme Judicial Court, which concluded that the principles developed under *Aguilar v. Texas*, 378 U.S. 410 (1960), provide a more appropriate structure for probable cause inquiries. *Id.* “[P]robable cause requires a substantial basis, for concluding that the items sought are related to the criminal activity under investigation, and that they reasonably may be expected to be located in the place to be searched at the time the search warrant issues.” *Commonwealth v. Kaupp*, 453 Mass. 102, 110 (2009).

The validity of this warrant rests on the sufficiency of the statements appearing on the face of the affidavit to support a finding of probable cause to believe that any of the articles or items specified in the would be found in the targeted location at the time of the warrant execution. See, e.g., *Commonwealth v. Reynolds*, 374 Mass. 142 (1977). The affidavit must be measured only from

what it contains within the four corners of the affidavit submitted in support of the application for the search warrant. *Commonwealth v. Kaupp*, 453 Mass. 102, 107 (2009). Moreover, the affidavit must satisfy the requirements of G.L. c. 276, Sec. 1-30 as amended, decisions of the Supreme Judicial Court and other courts of the Commonwealth, and the Constitutions of the United States as well as of the Commonwealth. See generally *Massachusetts Practice*, 2d ed., Vol. 30, Sec. 184; accord, *Commonwealth v. Upton*, 394 Mass. 363 (1985). Statements not appearing in the application cannot be considered in support of the warrant, as those statements were not before the magistrate who issued the warrant. *Commonwealth v. Reynolds*, 374 Mass. 142, 148 (1977).

The affidavit in this case provided insufficient probable cause because there was insufficient evidence to tie the criminal activity discussed in the affidavit to the actual residence of 231 Sunset Hill. Specific details are required to establish something more than simply "strong reason to suspect," which is not sufficient for probable cause. *Commonwealth v. Upton*, 394 Mass. 363, 370 (1985).

In *Pina*, the warrant affidavit included the following information:

(i) the confidential informant had engaged in a number of prior purchases from the defendant; (ii) in those prior purchases, the informant and the defendant followed a common method in which the informant called a specified telephone number, the defendant specified a location at which the informant should meet the defendant, and the two would thereafter meet at the location for the purpose of consummating the sale; (iii) on the occasion of the controlled purchase arranged by police, the informant followed the same practice, and police observed the defendant leave his apartment upon receiving the informant's call and drive directly to the location of the controlled purchase; (iv) police surveillance and investigation had established that the defendant resided in the apartment; and (v) the affiant police officer (with considerable experience in the methods and practices of drug delivery services) expressed his awareness that such services operate in the manner described in the affidavit for the purpose of keeping drug sales and deliveries away from the location at which the drugs are stored.

Commonwealth v. Pina, 71 Mass. App. Ct. 653, 657 (2008). Additionally, the affidavit in *Pina* indicated that the defendant had been observed by the police driving from his home to the location of a controlled buy and subsequently observed by the police returning home. *Id.*

Nevertheless, the Supreme Judicial Court suppressed the evidence seized as a result of executing the search warrant in the residence because they found insufficient nexus between the alleged criminal activity and the place of residence. *Pina*, 453 Mass. 441-42. Despite all of the above information included in the affidavit, the court in *Pina* held that the affidavit provided insufficient details tending to demonstrate that the defendant sold drugs from his apartment or that he kept his supply of drugs there. *Id.* at 442.

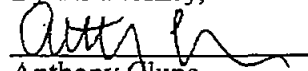
The warrant affidavit in the instant case is as insufficient as the affidavit in *Pina* because it fails to provide sufficient details suggesting that child pornography would be found at 231 Sunset Hill. [C]omputer technology has rendered the collection, storage, and dissemination of child pornography more amorphous. *Commonwealth v. Anthony*, 451 Mass. 59, 73 (2008). Nonetheless, all that is required is the consistent application of our well-established approach to analyzing the four corners of an affidavit for determining whether probable cause exists for a search warrant to issue. *Id.*

The police never established that the subscriber of the internet had any connection to 231 Sunset Hill. The affidavit states that the subscriber's mother resided at the address. Additionally, there is nothing to suggest in the affidavit that the IP address was part of closed network. Wi-fi internet is extremely commonplace in today's society. A wireless network that is unsecured would be able to be accessed from other units in a housing development. The affidavit provides a basis to suspect criminal activity, but falls short of establishing probable cause.

Conclusion

For all of the foregoing reasons, the defendant requests that this Honorable Court rule that the affidavit and search warrant were legally insufficient and that all evidence seized pursuant thereto be suppressed.

Adalberto Martinez,
By his attorney,



Anthony Olune
BBO # 663166
448 County Street
New Bedford, MA 02748
(508) 999-4088

Date: August 15, 2014

COMMONWEALTH OF MASSACHUSETTS

BRISTOL, ss.

FALL RIVER DISTRICT
COURT
NO. 1232CR02700

COMMONWEALTH

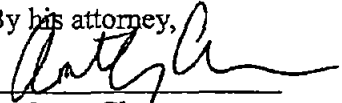
v.

ADALBERTO MARTINEZ

NOTICE OF APPEAL

The defendant gives notice, pursuant to Rule 3 of the Massachusetts Rules of Appellate Procedure, of his intent to appeal certain opinions, rulings, directions and judgments of the Court in the above entitled matter.

Adalberto Martinez,
By his attorney,

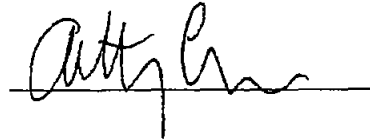

Anthony Clune
BBO # 663166
448 County St.
New Bedford, MA 02748
(508) 999-4088

Date: November 18, 2014

NOV 18 2014
Filed in court
(AP)

CERTIFICATION

I hereby certify that on the 18th day of November, 2014, I hand delivered a true and accurate copy of the within Notice of Appeal to an agent of the Bristol County District Attorney's Office, 888 Purchase St., New Bedford.

A handwritten signature in cursive script, appearing to read "Atty Gen", is written over a horizontal line.

UNITED STATES OF AMERICA, Plaintiff,

v.

GARY REIBERT, Defendant.

No. 8:13CR107.

United States District Court, D. Nebraska.

January 27, 2015.

MEMORANDUM AND ORDER

JOSEPH F. BATAILLON, Senior District Judge.

This matter is before the court on defendant Gary Reibert's objection, Filing No. 350, to the Findings and Recommendation ("F&R") of the United States magistrate judge, Filing No. 347, on Reibert's motion to suppress evidence found in a search of his residence on April 8, 2013.^[1] Filing No. 117. Reibert is charged in the Second Superseding Indictment with the receipt and attempted receipt of child pornography (Count I) in violation of 18 U.S.C. § 2252A(a)(2) and (b)(1) and the accessing of a computer in interstate commerce with the intent to view child pornography (Count II) in violation of 18 U.S.C. § 2252A(a)(5)(B) during the period of November 16, 2012, and December 2, 2012. See Filing No. 110, second superseding indictment.

In his motion to suppress defendant Reibert challenges two search warrants, one authorizing the government to install a Network Investigation Technique ("NIT") on a seized computer, and one authorizing the search of his residence.

Defendant Reibert objects to the magistrate judge's F&R, contending he was entitled to a *Franks* hearing^[2] on the issue of whether the affidavit in support of the warrant to employ the NIT failed to include evidence that negated probable cause. He also argues the government conducted a warrantless search of Reibert's computer by employing a NIT and contends he was entitled to present testimony of an expert, Tami Loehrs, on this issue. Further, he states the search warrant permitting the NIT was a general warrant and did not permit a search of Reibert's computer, nor was it a warrant authorizing a search of Reibert's computer. Last, he contends the warrant to search Reibert's residence and computer was not based upon probable cause.

Pursuant to 28 U.S.C. § 636(b)(1)(A), the court has conducted a de novo determination of those portions of the F&R to which the defendant objects. *United States v. Lothridge*, 324 F.3d 599, 600-01 (8th Cir. 2003). The court has reviewed the record, including the transcript of the suppression hearing, and the exhibits. See Filing No. 330, Transcript ("Tr."); Filing No. 164, Exs. 1-5; Filing No. 323, Exhibit List. The court accepts the facts set out by the magistrate judge and they need not be repeated here, except to the extent necessary to this court's findings. Filing No. 347, F&R at 2-4; Filing No. 330.^[3]

"In order to be entitled to a hearing under *Franks* the defendant must make a substantial preliminary showing of a false or reckless statement or omission and must also show that the alleged false statement or omission was necessary to the probable cause determination." *United States v. Crissler*, 539 F.3d 831, 833 (8th Cir. 2008) (quoting *United States v. Milton*, 153 F.3d 891, 896 (8th Cir. 1998)). This burden is "not easily [met]." *United States v. Engler*, 521 F.3d 965, 969 (8th Cir. 2008); see also *United States v. Stropes*, 387 F.3d 766, 771 (the defendant must show that the alleged omission would have made it impossible to find probable cause). "[I]f, when material that is the subject of the alleged falsity or reckless disregard is set to one side, there remains sufficient content in the warrant affidavit to support a finding of probable cause, no hearing is required." *Franks*, 438 U.S. at 171-72.

The court agrees with the magistrate judge's conclusion that defendant Reibert failed to make the substantial preliminary R. A. / 52

showing that law enforcement intentionally or recklessly omitted information from the warrant affidavit so as to entitle him to a *Franks* hearing. The defendant argues, in effect, that the government did not disclose in affidavits that it had installed a "trojan, in essence a virus, onto [defendant Reibert's] computer." Filing No. 330, Tr. at 14. The defendant made an offer of proof on the expert testimony it would proffer in support of that contention. *Id.* at 16-28. The court has reviewed the offer of proof and agrees with the magistrate judge that it does not satisfy the heavy burden of showing an intentional falsehood or omission. The court finds no error in the magistrate judge's denial of defendant Reibert's motion for a *Franks* hearing.

Further, the court has reviewed the warrant applications and agrees with the magistrate judge that the warrants were supported by probable cause. See Filing No. 164, Index of Evid., Exs. 1 & 2, search warrant applications and affidavits (sealed). "Probable cause exists when a 'practical, common-sense' inquiry that considers the totality of the circumstances set forth in the information before the issuing judge yields a 'fair probability that contraband or evidence of a crime will be found in a particular place.'" United States v. Stevens, 530 F.3d 714, 718 (8th Cir. 2008) (quoting Illinois v. Gates, 462 U.S. 213, 238 (1983)). Reibert contends that the expert testimony of Tami Loehrs, a purported computer forensics expert, would establish that the court-authorized deployment of the NIT constituted a warrantless search of his computer "that went into [the defendant's] house, modified the workings of his computer, in order to send back data to the government." Filing No. 330, Tr. at 4. The magistrate judge sustained the government's objection to the expert's testimony on *Daubert* grounds, but allowed an offer of proof with respect to her testimony.^[4] Filing No. 330, Transcript at 19-22, 24-28. The court finds no error in the magistrate judge's *Daubert* ruling. Loehrs conceded that she "had no idea" whether "the investigative technique returned any more information than it was authorized." *Id.* at 27-28. She also conceded that flash applications are present on many websites and flash applications can reveal the IP and user. *Id.* at 28. Even if allowed, her testimony does little to undermine the information contained in the affidavit that supports the NIT warrant.

The magistrate judge found the affidavits of Special Agents Jeffrey Tarpinian and Andrea Kenzig provided probable cause for the searches and the court agrees. See F&R at 5-6; Filing No. 164, Index of Evid., Exs. 1 & 2. The affidavit in support of the application for a NIT described the investigation, the TOR network, and target website in detail, including the website's function in advertising and distributing child pornography, and also related the types and amount of child pornography available on the site, including sections specific to babies and prepubescent boy and girls. *Id.*, Ex. 1 at 12-29. It also described the law enforcement investigation that led investigators to the website. See Filing No. 164, Ex. 2 at 9-13, 15-20. It also describes the operation to the NIT. *Id.* at 29-32. The warrant authorized the use of a NIT (computer code) to be deployed on the computer server that operated TOR network "Bulletin Board A," then located at a government facility, in order to obtain information, including IP addresses, from computers accessing images on Bulletin Board A or sending or viewing private messages on Bulletin Board A. *Id.* at 39, 44. The affidavit in support of the residential warrant detailed the investigative techniques used to identify Reibert and connect him to the website. Filing No. 164, Ex. 2, Affidavit at 9-15. The affiant states a person with an IP address issued to Reibert accessed the website at issue and specifies and describes the images that were accessed. *Id.* at 16-20. Those facts, together with the affiant's expertise regarding the characteristics of child pornography consumers, supports a fair probability that child pornography would be found on one or more computers at his residence. *Id.* at 22-26.

In the Eighth Circuit, for the purposes of determining whether probable cause exists to search a computer, an IP address assigned to a specific user at the time illegal internet activity associated with that IP address occurs is a sufficient basis to find a nexus between the unlawful use of the internet at that IP address and a computer possessed by the subscriber assigned the address. See, e.g., United States v. Stults, 575 F.3d 834, 843-44 (8th Cir. 2009) (holding that probable cause supported warrant where officers used IP address to identify possessor of child pornography on a filesharing network); United States v. Perrine, 518 F.3d 1196, 1205-06 (10th Cir. 2008) (upholding probable cause where pornographic images were traced to defendant's residence using IP address); United States v. Perez, 484 F.3d 735 (5th Cir. 2007) (the IP address provided "a substantial basis to conclude that evidence of criminal activity" would be found at the defendant's home, even if it did not conclusively link the pornography to the residence); United States v. Wagers, 452 F.3d 534, 539 (6th Cir. 2006) (upholding probable cause where suspect was identified as a member of child pornography websites through an IP address assigned to his residence); United States v. Hay, 231 F.3d 630, 635-

36 (9th Cir. 2000) (finding a substantial basis for magistrate's probable cause determination where images of child pornography were traced to defendant using an IP address).

Further, even if the information submitted to support the issuance of a search warrant did not amount to probable cause, the good faith exception to the exclusionary rule identified in United States v. Leon, 468 U.S. 897, 922 (1984), would apply. "Under the *Leon* good-faith exception, disputed evidence will be admitted if it was objectively reasonable for the officer executing a search warrant to have relied in good faith on the judge's determination that there was probable cause to issue the warrant." United States v. Grant, 490 F.3d 627, 632 (8th Cir. 2007). Even if the Court were now to conclude here that the affidavit supporting the search warrant did not set forth facts sufficient to demonstrate probable cause to search the computers at defendant Reibert's residence, on the present record, law enforcement's good-faith reliance on the warrants issued by the magistrate judge to search those computers militates against suppressing any evidence obtained in the search. See Leon, 468 U.S. at 919-921 (exclusionary rule does not apply "when an officer acting with objective good faith has obtained a search warrant from a judge or magistrate and acted within its scope").

Accordingly, the court concludes that the defendant's objections to the F&R should be overruled, the magistrate judge's F&R should be adopted and the defendant's motion to suppress should be denied.

IT IS ORDERED:

1. Defendant Reibert's objections to the F&R (Filing No. 350) are overruled.
2. The Findings and Recommendation of the magistrate judge (Filing No. 347) is hereby adopted.
3. Defendant Reibert's motion to suppress (Filing No. 117) is denied.

[1] The portion of the defendant's motion challenging the admissibility of his statements was withdrawn at the evidentiary hearing. See Filing No. 330, Transcript at 33-35; Filing No. 347, F&R at 1 n.1. Also, the defendant's challenge to the delayed notice of the warrant was denied after an omnibus evidentiary hearing in an order dated October 14, 2014. See Filing No. 294, Memorandum and Order at 7-8, 10.

[2] See *Franks v. Delaware*, 438 U.S. 154, 178 (1978) (holding that, under certain limited circumstances, a defendant is entitled under the Fourth Amendment to collaterally attack the veracity of a warrant affidavit in the context of challenging the existence of probable cause).

[3] See also Filing No. 254, F&R at 5-7 (background facts involving government's investigation of "Website A" and the onion router (TOR) software).

[4] *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579 (1993).

Save trees - read court opinions online on Google Scholar.

COMMONWEALTH,
vs.
JOSIAH H. CANNING.

No. SJC-11773.

Supreme Judicial Court of Massachusetts, Barnstable.

January 8, 2015.

April 27, 2015.

Elizabeth A. Sweeney, Assistant District Attorney, for the Commonwealth.

Richard F. Comenzo for the defendant.

The following submitted briefs for amici curiae:

John M. Collins for Massachusetts Chiefs of Police Association, Inc.

Paul R. Rudof, Committee for Public Counsel Services, for Daniel J. Chao & another.

Steven S. Epstein & Marvin Cable for National Organization for the Reform of Marijuana Law.

Present: Gants, C.J., Spina, Cordy, Botsford, Duffly, Lenk, & Hines, JJ.

BOTSFORD, J.

We consider here for the first time the Commonwealth's new medical marijuana law, "An Act for the humanitarian medical use of marijuana," St. 2012, c. 369 (act), which the voters approved in November, 2012.^[1] The central question presented is whether, with the act in effect, police may obtain a search warrant to search a property where they suspect an individual is cultivating marijuana by establishing probable cause that cultivation is taking place or are required to establish probable cause to believe that the individual was not registered, or licensed, to do so. In accord with cases relating to other types of license regimes, we conclude that, if police seek a warrant to search such a property for evidence of illegal marijuana possession or cultivation, they must offer information sufficient to provide probable cause to believe the individual is not properly registered under the act to possess or cultivate the suspected substance. In this case, a judge in the District Court allowed the defendant's motion to suppress evidence seized by police during a search of the defendant's property conducted pursuant to a warrant in May of 2013, after the act went into effect. We agree with the motion judge that the affidavit filed in support of the search warrant application demonstrated probable cause that the defendant was cultivating marijuana at the property, but that, in light of the act, the affidavit failed to establish probable cause to believe that the defendant was not authorized to do so and therefore was committing a crime. We affirm the order allowing the motion to suppress.^[2]

Background.

On May 30, 2013, a three-count complaint issued from the Orleans Division of the District Court Department charging the defendant, Josiah H. Canning, with possession with the intent to distribute marijuana, G. L. c. 94C, § 32C (a); distribution of marijuana, G. L. c. 94C, § 32C (a); and conspiracy to violate the drug laws, G. L. c. 94C, § 40.^[3] The complaint's issuance followed a search of the defendant's property in Brewster conducted May 30, 2013, pursuant to a search warrant issued on May 29. The affidavit submitted by Detective Christopher Kent of the Yarmouth police department in support of the warrant application recited the following facts.

During the week of May 19, 2013, Kent met with a confidential informant, who told Kent that the owner of certain property in Brewster (property) — whom Kent later determined from town records to be the defendant — and another male were involved in an indoor "marijuana grow" operation located at the property.^[4] On May 21, Kent and another detective observed the property from a nearby driveway, and noticed that windows of the addition to the house on the property were obscured by dark material, saw an aluminum flexible hose protruding out of one of the windows, and also observed a pickup truck registered to the defendant in front of the house. On May 24 and 28, Kent and one or more additional police officers returned to observe the property; on both occasions, they smelled a strong odor of "freshly cultivated" marijuana emanating from the house, noticed the aluminum hose coming out of the window of the addition, heard the sound of fans, and, using night vision goggles, saw light emanating from another window. Also on May 28, Kent was provided information from a police officer in another town that that officer previously had observed the defendant and another man purchasing "a large amount of indoor [marijuana] grow materials" from a "hydroponic shop" in Foxborough and then loading the materials into an automobile registered to the defendant. On May 29, Kent obtained utility bills relating to electrical service for the property and neighboring homes on Main Street in Brewster. These records revealed that for the previous six months, the average kilowatt usage for three neighboring homes was 542.3 kilowatt hours (kWh), 23.3 kWh, and 246.6 kWh, respectively; the average kilowatt usage for the defendant's property for the same time period was 3,116.5 kWh. Based on his training and experience, Kent was aware that because marijuana growing operations require different types of electrical equipment, e.g., "high intensity discharge lamps, fluorescent lights, fans, reflectors, irrigation and ventilation equipment such as aluminum flexible hose" to be operating consistently, high usage of electricity — a "noticeable increase in kilowatt usage" — is to be expected.

When the police executed the search warrant that, based on the affidavit, a judge in the District Court had issued, the defendant was present. Seized during the search, among other items, were seventy marijuana plants, eleven fluorescent industrial lights, an aluminum flexible hose, a digital scale, approximately 1.2 pounds of marijuana, and \$2,697. The defendant was placed under arrest.

The defendant filed a motion to suppress the seized evidence, and also to suppress statements he made at the time of the search and his arrest. A different District Court judge allowed the motion in a written memorandum of decision. The judge concluded that the search warrant affidavit "establishe[d] probable cause that marijuana was being cultivated indoors at the defendant[']s home," but concluded in substance that in light of the act, the affidavit failed to establish probable cause that the cultivation was for more than a sixty-day supply of marijuana or that the defendant was not authorized to grow that amount — and therefore that the cultivation was illegal. The Commonwealth filed a timely application for leave to file an interlocutory appeal of the judge's suppression order and motion to stay further proceedings in the case. See Mass. R. Crim. P. 15 (a) (2), as appearing in 422 Mass. 1501 (1996). A single justice of this court allowed the application and reported the case to the Appeals Court. Thereafter, we allowed the Commonwealth's motion for direct appellate review.

Discussion.

1. Overview of the act.

The voters approved the act as a ballot measure in 2012, and the act went into effect on January 1, 2013. St. 2012, c. 369. Section 1 of the act sets out a statement of purpose:

"The citizens of Massachusetts intend that there should be no punishment under state law for qualifying patients, physicians and health care professionals, personal caregivers for patients, or medical marijuana treatment center agents for the medical use of marijuana, as defined herein" (emphasis added).

The term "medical use of marijuana" is defined in the act as follows:

"Medical use of marijuana" shall mean the acquisition, cultivation, possession, processing (including development of related products such as food, tinctures, aerosols, oils, or ointments), transfer,

transportation, sale, distribution, dispensing, or administration of marijuana, for the benefit of qualifying patients in the treatment of debilitating medical conditions, or the symptoms thereof" (emphasis added).

St. 2012, c. 369, § 2 (I). The substantive provisions of the act that follow the definitional section first set out the parameters of protection from State prosecution and penalties that the act respectively gives to physicians and health care professionals, qualifying patients and their personal caregivers, and licensed dispensary agents. See *id.* at §§ 3-5. ^[5] See also *id.* § 6 (A) ("The lawful possession, cultivation, transfer, transport, distribution, or manufacture of medical marijuana as authorized by this law shall not result in the forfeiture or seizure of any property"). These provisions are followed by a section specifying "limitations" of the act, including the following: "Nothing in [the act] supersedes Massachusetts law prohibiting the possession, cultivation, transport, distribution, or sale of marijuana for nonmedical purposes." *Id.* at § 7 (E). Thereafter, the act establishes a medical marijuana registration or licensing regime that is to be set up and administered by the Department of Public Health (department), and that covers nonprofit medical marijuana treatment centers, medical marijuana center dispensary agents, and qualifying patients and personal caregivers. See *id.* at §§ 9-12. Under the act, it is clear that the principal source of medical marijuana is intended to be the nonprofit medical marijuana treatment centers, or dispensaries, that are to be registered by the department. See *id.* at §§ 2 (H), 9 (B), (C). To that end, the act directed that during the first year the act was in effect, the department "shall" have registered up to thirty-five of these centers, with at least one in every county, and further states that "[i]n the event the [d]epartment determines in a future year that the number of treatment centers is insufficient to meet patient needs, the [d]epartment shall have the power to increase or modify the number of registered treatment centers. See *id.* at § 9 (C).

Of particular relevance here are the act's provisions relating to qualifying patients and personal caregivers as well as to hardship cultivation registrations. A "qualifying patient" is defined as "a person who has been diagnosed by a licensed physician as having a debilitating medical condition." St. 2012, c. 369, § 2 (K). The act requires a qualifying patient as well as a personal caregiver^[6] to obtain from the department a "registration card," which is a personal identification card issued by the department that serves both to "verify that a physician has provided a written certification to the qualifying patient," and to "identify for the [d]epartment and law enforcement those individuals who are exempt from Massachusetts criminal and civil penalties for conduct pursuant to the medical use of marijuana." *Id.* at § 2 (L). See *id.* at § 12 (describing application requirements for medical marijuana registration card for qualifying patients and personal caregivers). A qualifying patient or his or her personal caregiver is permitted to possess up to a sixty-day supply of marijuana necessary for the patient's personal medical use. See *id.* at § 4 (A). In addition, a qualifying patient whose access to a licensed medical marijuana treatment center is limited by finances or an inability to travel to a licensed center may obtain a "hardship cultivation registration" that allows the patient or the patient's personal caregiver to cultivate a sufficient number of marijuana plants to produce and maintain a sixty-day supply of marijuana. *Id.* at § 11. The act tasks the department with defining "the quantity of marijuana that could reasonably be presumed to be a sixty-day supply for qualifying patients." *Id.* at § 8.^[7]

The act provides that the department was to issue regulations to govern implementation of all the registration provisions in the act. St. 2012, c. 369, § 13. These regulations were to be published within 120 days of the act's effective date, May 1, 2013. The act also provides, however, that "[u]ntil the approval of final regulations, written certification by a physician shall have constituted a registration card for a qualifying patient." *Id.* See *id.* at § 2 (N) (definition of "written certification"). Additionally, until final regulations were in place, "the written recommendation of a qualifying patient's physician shall have constituted a limited [i.e., hardship] cultivation registration." *Id.* at § 11.^[8]

The department issued its final medical marijuana regulations on May 8, 2013. 105 Code Mass. Regs. § 725.000 (2013). But of significance to the present case, § 725.015 of these regulations, which defines the registration requirements for a qualifying patient, provides that if a qualifying patient received an initial written certification signed by a physician before the department was accepting registration applications, "the initial certification will remain valid until the application for the registration card is approved or denied by the [d]epartment."^[9] The same holds true for limited cultivation registrations: a qualifying patient who received written certification from a physician is entitled to continue to use that written certification as a hardship cultivation registration "until the application for the hardship cultivation registration card is approved or denied by the [d]epartment." 105 Code Mass. Regs. § 725.035(L) (2013). The parties do not dispute that

at the time of the search of the property, the department was not yet approving or denying any applications for registration, and there were no registered medical marijuana treatment centers in operation.^[10] Thus, a qualified physician's written recommendation, undocumented in any database, sufficed as both a medical marijuana registration card and a limited medical marijuana cultivation registration.

2. Search warrant and application.

"Our inquiry as to the sufficiency of the search warrant application always begins and ends with the four corners of the affidavit. . . . The magistrate considers a question of law: whether the facts presented in the affidavit and the reasonable inferences therefrom constitute probable cause. . . . [W]e determine whether, based on the affidavit in its entirety, the magistrate had a substantial basis to conclude that a crime had been committed, . . . and that the items described in the warrant were related to the criminal activity and probably in the place to be searched" (quotations and citations omitted). Commonwealth v. O'Day, 440 Mass. 296, 297-298 (2003). See Commonwealth v. Donahue, 430 Mass. 710, 711-712 (2000).

The Commonwealth contends that Kent's affidavit established probable cause for the search because, as the motion judge concluded, the affidavit provided probable cause to believe that the defendant was engaged in cultivating marijuana at the property, and in the Commonwealth's view all-or-any cultivation of marijuana remains illegal even under the act. To the extent that the act permits a limited class of properly licensed or registered persons to grow marijuana, the argument continues, the existence of a license or registration is an affirmative defense for a defendant charged with unlawful cultivation to raise at trial — the Commonwealth is not obligated to disprove such a status in order to conduct a search at the outset of an investigation.

We disagree. Although as a general matter, marijuana cultivation is a crime, see G. L. c. 94C, § 32C (a); Commonwealth v. Palmer, 464 Mass. 773, 777 (2013), and the act specifies generally that it remains so, see St. 2012, c. 369, § 7 (E), the Commonwealth is incorrect that the act has not effected any change in the statutory and regulatory landscape relevant to establishing probable cause for a search targeting such cultivation. What § 7 (E) states is that nothing in the act "supersedes Massachusetts law prohibiting the . . . cultivation . . . of marijuana for nonmedical purposes" (emphasis added). Under the act, cultivation of marijuana is expressly permitted if a person or entity is properly registered to do so, and the cultivation does not exceed the amount necessary to yield a sixty-day supply of medical marijuana. See St. 2012, c. 369, §§ 9 (B), (D), 11. See also *id.* at §§ 4-6. As previously stated, when the search at issue here took place, the act was not fully implemented; no marijuana treatment centers were operating; and therefore, pursuant to the act's express provisions, see *id.* at §§ 11, 13, every person who was certified as a qualifying patient or the patient's personal caregiver was authorized to cultivate a sufficient quantity of marijuana to produce a sixty-day supply — presumptively ten ounces.

In these circumstances, as the motion judge suggested, our cases involving searches for firearms that may be legally possessed with a license but are illegal in the absence of one provide an appropriate analytic framework. See Commonwealth v. Toole, 389 Mass. 159, 163 (1983).^[11] Accord Commonwealth v. Nowells, 390 Mass. 621, 627 (1983) (search warrant affidavit did not establish probable cause for search of defendant's apartment for illegal firearms where informants only indicated they had seen guns there: "The ownership or possession of a handgun [or a rifle] is not a crime and standing alone creates no probable cause"). See also Commonwealth v. Couture, 407 Mass. 178, 181, cert. denied, 498 U.S. 951 (1990); Commonwealth v. Stevens, 361 Mass. 868 (1972). As these cases indicate, although firearms cannot legally be carried without a license to carry, see G. L. c. 269, § 10 (a), in the absence of any evidence beyond the "unadorned fact," Couture, *supra*, that the defendant was carrying a gun, there was no probable cause to suspect a crime was being committed.^[12] Cf. Commonwealth v. Marra, 12 Mass. App. Ct. 956, 956-957 (1981) (defendant convicted of storing dynamite without license; conviction reversed where search warrant authorizing search of defendant's trailer for dynamite was not based on probable cause: "The observation of a box containing [dynamite] blasting caps, without more, to indicate that their storage was unlicensed, does not provide probable cause for entry into the [defendant's] trailer" where no circumstances set out in affidavit indicated blasting caps were, or were reasonably

likely to be, unlicensed).

The Commonwealth again misses the mark in seeking to distinguish these cases and arguing that the existence of a registration card or written certification, like the existence of a license, constitutes an affirmative defense that the defendant himself is obliged to raise in the first instance — at trial. A license does constitute an affirmative defense at trial to be raised by the defendant. See G. L. c. 278, § 7.^[13] See also Commonwealth v. Gouse, 461 Mass. 787, 804-808 (2012); Couture, 407 Mass. at 181-182; Commonwealth v. Jones, 372 Mass. 403, 405-406 (1977). But this case is not about defenses at trial; the issue is probable cause to conduct an investigatory search. At the trial of a case in which the existence or nonexistence of a license defines whether the charged conduct was legal or instead a crime, as Couture explains, the defendant "has every opportunity to respond" by producing the license authorizing his conduct, and in the absence of the defendant's doing so, it is not unfair for the jury to presume in accordance with c. 278, § 7, that the defendant did not have a license. Couture, *supra* at 182. Accord Gouse, *supra* at 806. At the time of a search, however, such a defendant is in a very different position: the police arrive, armed with (among other things) a warrant authorizing the search; the defendant has no right to object or respond, and indeed may not even be present. Cf. Couture, *supra* at 182-183 (contrasting position of defendant at trial with defendant's position when confronted by police stopping defendant's truck, removing him from it at gunpoint, and conducting warrantless search of truck to locate pistol police suspected would be present). Cf. also Commonwealth v. Landry, 438 Mass. 206, 211 (2002) (charge of unlawful possession of hypodermic needle; contrasting defendant's burden to raise affirmative defense of license at trial with question whether probable cause existed for unlawful possession at time of arrest).^[14]

The firearms and other license cases just discussed govern the result here. Beginning with the initial statement of purpose, the act's provisions make it abundantly clear that its intent is to protect the lawful operation of the medical marijuana program established by the legislation from all aspects of criminal prosecution and punishment, including search and seizure of property as part of a criminal investigation. See St. 2012, c. 369, §§ 1, 3-6. The act's medical marijuana program is structured as a licensing or registration system, and expressly contemplates the lawful possession, cultivation, and distribution of marijuana for medical purposes by a number of different individuals (and certain nonprofit entities), as long as they are registered to do so. In light of the statutory and regulatory framework created by the act, a search warrant affidavit setting out facts that simply establish probable cause to believe the owner is growing marijuana on the property in question, without more, is insufficient to establish probable cause to believe that the suspected cultivation is a crime. Missing are facts indicating that the person owning or in control of the property is not or probably not registered to cultivate the marijuana at issue.^[15]

Detective Kent's affidavit filed in support of the search warrant in this case did not contain any information at all addressing whether the defendant was or was not registered as a qualifying patient or personal caregiver to grow the marijuana the police reasonably suspected was growing on the property.^[16] Nor, as the motion judge observed, did it contain other facts or qualified opinions that might supply an alternate basis to establish the necessary probable cause to believe the cultivation was unlawful. See note 15, *supra*. As such, the affidavit failed to establish probable cause for the search.^[17]

We disagree with the Commonwealth that the result we reach imposes an impossible burden on police to search for elusive and difficult-to-locate information about whether a person suspected of growing marijuana is registered to do so. Although not available in 2013 when the search here was conducted, we assume that with the introduction of the electronic registration system, see note 10, *supra*, there is or soon will be available to law enforcement officers an accessible list of "the persons issued medical marijuana registration cards" as provided in § 15 of the act.^[18] Moreover, as we have suggested (see note 15, *supra*), information independent of registration status may also be presented to establish probable cause concerning the suspected unlawful cultivation of marijuana.

Conclusion.

So ordered.

[1] The measure was placed before the voters at the Statewide election held November 6, 2012, pursuant to art. 48, *The Initiative*, Part V, § 1, amended by art. 81, § 2, of the Amendments of the Massachusetts Constitution.

[2] We acknowledge the amicus briefs submitted by Daniel J. Chao and Shawn P. Kelly and by the National Organization for the Reform of Marijuana Laws, in support of the defendant; and the Massachusetts Chiefs of Police Association, Inc., in support of the Commonwealth.

[3] For reasons that have not been explained, the defendant was not charged with unlawful cultivation of marijuana. There does not appear to be any evidence of distribution in this case.

[4] The property consists of a house with a small addition to the rear (connected by a breezeway), a barn in the front yard, and a large barn in the back yard.

[5] Pertinent to this case is § 4 of St. 2012, c. 369 (act):

"Protection From State Prosecution and Penalties for Qualifying Patients and Personal Caregivers

"Any person meeting the requirements under this law shall not be penalized under Massachusetts law in any manner, or denied any right or privilege, for such actions.

"A qualifying patient or a personal caregiver shall not be subject to arrest or prosecution, or civil penalty, for the medical use of marijuana provided he or she:

"(a) Possesses no more marijuana than is necessary for the patient's personal medical use, not exceeding the amount necessary for a sixty-day supply; and

"(b) Presents his or her registration card to any law enforcement official who questions the patient or caregiver regarding use of marijuana."

[6] A "personal caregiver" is defined to mean "a person who is at least twenty-one (21) years old who has agreed to assist with a qualifying patient's medical use of marijuana." St. 2012, c. 369, § 2 (J).

[7] Under the medical marijuana regulations of the Department of Public Health (department), discussed in the next paragraph of the text, the presumptive sixty-day supply of medical marijuana is defined as ten ounces. See 105 Code Mass. Regs. § 725.004 (2013). The sixty-day supply may be greater than ten ounces for an individual qualifying patient upon the patient's certifying physician providing written certification and documentation that a greater supply is necessary. See 105 Code Mass. Regs. § 725.010(l) (2013). The regulation does not identify the number of marijuana plants that may be necessary to grow ten ounces of marijuana.

[8] It appears that the act uses the terms "certification" and "recommendation" interchangeably. Reading together the quoted provisions of St. 2012, c. 369, §§ 13 and 11, relating to what respectively constitutes a qualifying patient's registration card and a hardship cultivation registration pending approval of the department's regulations, we understand them to be referring to the same document, namely, the "written certification" defined in St. 2012, c. 369, § 2 (N), that is signed by a licensed physician and certifies the qualifying patient for use of medical marijuana. A memorandum appearing on the department's Web site concerning implementation of the act confirms this understanding. See "Guidance for Law Enforcement Regarding the Medical Use of Marijuana," Department of Public Health, Bureau of Health Care Safety and Quality, *Medical Use of Marijuana Program*, at 2 (Updated Apr. 15, 2015) ("Until [the department] begins to process hardship cultivation applications, patients or their caregivers may conduct limited cultivation at their primary residence, but may only grow a sufficient amount for their sixty day supply as certified by the patient's physician").

[9] There is a separate provision governing the registration requirements for personal caregivers, 725 Code Mass. Regs. § 725.020 (2013), and it also provides that "the initial certification will remain valid until the application for the registration card is approved or denied by the [d]epartment." *Id.* at § 725.020(C).

[10] According to its public announcements, the department has determined that the registration process should be electronic. See Program Update — October 8, 2014, Information for Patients and Caregivers, Massachusetts Department of Public Health, <http://www.mass.gov/eohhs/gov/departments/dph/programs/hcq/medical-marijuana/patients-and-caregivers.html> [<http://perma.cc/7GS7-ADNU>]. The department's goal of having the electronic registration system ready by January, 2014, see 105 Code Mass. Regs. §§ 725.015(C), 725.020(C), 725.035(L) (setting initial registration deadline at January 1, 2014), went unrealized. On October 8, 2014, the department announced that, effective February 1, 2015, "paper certifications" by physicians would no longer be valid proxies for proper registration and, as of that date, every qualifying patient would be required to obtain an electronic certification from his or her physician and to be formally and electronically registered with the department. See Program Update — October 8, 2014, Information for Patients

and Caregivers, *supra*.

[11] In *Toole*, we considered a warrantless search of a vehicle in which police suspected a gun was located: "[I]t has not [been] shown that, when the search was conducted, the police reasonably believed that there was a connection between the vehicle and any criminal activity of the defendant, an essential element to a finding of probable cause. . . . The empty holster and ammunition found on the defendant certainly created probable cause to believe that there was a gun in the cab. But carrying a .45 caliber revolver is not necessarily a crime. A possible crime was carrying a gun without a license to carry firearms, G. L. c. 269, § 10 (a). However, the police did not learn that the defendant had no firearm identification card until after the search. They apparently never asked the defendant whether he had a license to carry a firearm" (citation omitted). Commonwealth v. Toole, 389 Mass. 159, 163 (1983).

[12] Commonwealth v. Gouse, 461 Mass. 787 (2012), a case on which the Commonwealth relies, is inapposite. In *Gouse*, the defendant attacked the victim, his former girl friend, on the street and left the scene; the investigating police were told by bystanders as well as the defendant's father that he might be armed; the police also had information that he had been released recently from prison, and had been observed armed with a weapon and dealing "crack" cocaine. *Id.* at 788, 790-791. On the same day as the attack of the victim, the defendant was stopped by the police while driving in a vehicle, removed from the vehicle, and arrested, and the vehicle was impounded. *Id.* at 791. The police thereafter, during a warrantless search of the vehicle, found a gun in a bag that had been placed in the trunk of the vehicle. *Id.* at 791-792. Before trial, the defendant unsuccessfully moved to suppress evidence of the gun, but not on the ground that probable cause did not exist to believe he was not licensed to carry the weapon. See *id.* at 792-794. (Indeed, such an argument would have been highly problematic, given that the defendant at the time, in the court's words, was "a fleeing felon." See *id.* at 794. A felon, by definition, may not be licensed to carry a firearm. See G. L. c. 140, § 131 [d] [i].) The defendant in *Gouse* did raise a challenge related to the license issue, but the challenge concerned the allocation of the burden of proof between the defendant and the Commonwealth at trial concerning the existence of a license. See Gouse, *supra* at 799-808.

[13] General Laws c. 278, § 7, provides: "A defendant in a criminal prosecution, relying for his justification upon a license . . . shall prove the same; and until so proved, the presumption shall be that he is not so authorized."

[14] The Commonwealth cites five decisions from other States' courts as ostensibly persuasive authority that a medical marijuana license is exclusively an affirmative defense, rather than a legalizing mechanism for program participants. See *Niehaus vs. State*, Nos. A-8385, 4798 (Alaska Ct. App. Dec. 10, 2003); People v. Sexton, 296 P.3d 157 (Colo. App. 2012); *State vs. Meharg*, No. DC-06-16 (Mont. 21st Jud. Dist. Ct. May 26, 2006); State v. Senna, 194 Vt. 283 (2013); State v. Fry, 168 Wash. 2d 1, 13 (2010). We do not think these cases offer useful guidance here. The courts were considering substantially different medical marijuana laws, and also very different factual contexts.

[15] This is not to say that such an affidavit always must contain facts directly establishing that the person whose property the police seek to search for evidence of unlawful marijuana cultivation is or is probably not registered to do so; reasonable inferences may be drawn that a suspected marijuana cultivation operation is unlawful from other facts. For example, except for registered medical marijuana treatment centers, it remains unlawful to cultivate marijuana for sale. Facts indicating that a confidential informant recently purchased marijuana from the owner of the property where the cultivation operation is suspected to be taking place would likely supply the requisite probable cause to search that property for evidence of unlawful cultivation, as would information that police recently had observed marijuana plants growing on the property and that, in the opinion of a properly qualified affiant, the number of plants exceeded the quantity necessary to grow a sixty-day supply of ten ounces.

[16] From start to finish, the affidavit reads as though the act did not exist.

[17] In arguing against this conclusion, the Commonwealth relies heavily on Commonwealth v. Palmer, 464 Mass. 773, 775-778 (2013). The reliance is misplaced. In *Palmer*, we considered what impact, if any, the decriminalization of possession of one ounce or less of marijuana, a ballot measure approved by the voters in 2008, had on G. L. c. 94C, § 32C (a), which defines the offense of cultivation of marijuana. See Palmer, *supra* at 775. We concluded that the decriminalization measure did not affect the cultivation statute, and that cultivation of marijuana of one ounce or less remained a crime. *Id.* at 774, 777, 779. But the events giving rise to the criminal charges at issue in *Palmer* occurred in 2010, see *id.* at 774, no issue concerning the medical marijuana act, passed in 2012, was raised in *Palmer*, and the court did not consider the relationship of the medical marijuana act to § 32C (a) in any respect.

[18] Section 15 of the act states:

"The department shall maintain a confidential list of the persons issued medical marijuana registration cards. Individual names and other identifying information on the list shall be exempt from [G. L. c. 66, § 10, the Public Records Law], and not subject to disclosure, except to employees of the department . . . and to Massachusetts law enforcement officials when verifying a card holder's registration" (emphasis added).

6/26/2015

Commonwealth v. Canning, Mass: Supreme Judicial Court 2015 - Google Scholar

Save trees - read court opinions online on Google Scholar.

SYMPOSIUM: TRIAL 2010: A LOOK INSIDE OUR NATION'S COURTROOMS: TWENTIETH ANNUAL DEPAUL LAW
REVIEW SYMPOSIUM: COMMENT: BALANCING EXPECTATIONS OF ONLINE PRIVACY: WHY INTERNET
PROTOCOL (IP) ADDRESSES SHOULD BE PROTECTED AS PERSONALLY IDENTIFIABLE INFORMATION, 60
DePaul L. Rev. 895

Copy Citation

Spring, 2011

Reporter

60 DePaul L. Rev. 895

Length: 24941 words

Author: Joshua J. McIntyre*

* J.D. Candidate 2011, DePaul University College of Law; B.A. 2008, Saint Ambrose University. I would like to thank Associate Professor Matthew Sag of the Loyola University Chicago School of Law, whose guidance aided the direction of this Comment, as well as all of the Law Review members who have provided their excellent editorial assistance. I also want to thank my parents, David and Kimma McIntyre, and my fiancée, Ann Lamb, whose continued love and support have always kept me moving forward.

LexisNexis Summary

... Privacy law should not, therefore, protect IP addresses when they are not correlated to other PII, such as when they are maintained by Web site operators in normal network traffic logs. ... Many ISPs have no reason to fight these subpoenas and readily give up their subscribers' names, addresses, telephone numbers, and other identifying data without demanding any court oversight or providing any notice to the subscriber. ... An IP address is assigned to a computer or other device accessing the Internet and is communicated between devices as part of the normal data exchange. ... To date, Congress has rejected comprehensive privacy legislation in favor of a large collection of statutes, each of which protects specific types of information in particular circumstances. ... Giving Viacom access to such a database is not a trivial matter; and it deserved the court's considered analysis of whether Viacom's interest in tracking down copyright infringers outweighed the privacy interests of potentially millions of users who would be linked to the content they had viewed on the Web site.

Text

[895]

Introduction

About the time the Internet age began, [1] the Supreme Court upheld the First Amendment right to distribute anonymous political campaign handbills, [2] lauding anonymous free speech as "a shield from the tyranny of the majority." [3] Within two years, the Court had explicitly applied free speech to the new landscape of cyberspace. [4] The advent of the Internet had brought hope of a new public square for anonymous discourse, [5] a place where anyone with a computer and a phone line could speak openly to the entire world. [6]

Not two decades later, legal reality has dashed that utopian dream. Abuses of the anonymity that the Internet once afforded have required a balancing against other private rights, [7] and no longer is there a reasonable expectation of privacy in many Internet communications. [8] Instead, today's online world lulls its inhabitants into a false [896] sense of anonymity while secretly recording their every move for future discovery. [9]

This monitoring is made possible by the inherent structure of the Internet, the most crucial component of which is the simply named Internet Protocol (IP). [10] Every computer connected to the Internet receives a unique IP address that facilitates communications with other computers. [11] As part of the normal data exchange, these addresses are recorded, or "logged," by Web servers for future network and security analysis. [12] These logs, however, can also provide a breadcrumb trail of a user's online activity. [13] When a user views a Web site, a computer server logs his IP address. [14] When a user posts on a blog, [15] a server logs his IP address. [16] When a user views a sexually explicit photograph, [17] reads a political article, or searches for "bomb placement white house," [18] a server logs his IP address.

[897] Although these logs are scattered across the vast reaches of the Internet, [19] there are important middlemen with access to it all: Internet Service Providers (ISPs). [20] ISPs assign IP addresses to their subscribers, logging who is using what address at any given time. [21] ISPs are the gatekeepers of access to not only the Internet but also to the identification of any particular user. [22] By comparing its own IP address logs to those maintained by the Internet's Web servers, [23] an ISP can readily link online activity to a specific subscriber account and, potentially, [24] to an individual. [25] This means that ISPs "have the power to obliterate privacy online. Everything we say, hear, read, or do on the Internet first passes through ISP computers." [26]

Herein lies the concern for privacy. Although data logs maintained by Web site operators typically correlate online activity only to an IP address, that address may be

traced backwards to expose the individual behind the computer. [27] While various federal statutes protect similar data such as telephone numbers and mailing addresses as Personally Identifiable Information (PII), federal privacy law does not generally regard IP addresses as information worthy of protection. [28] It has, therefore, become commonplace for litigants to subpoena ISPs [898] to unmask online speakers. [29] Many ISPs have no reason to fight these subpoenas [30] and readily give up their subscribers' names, addresses, telephone numbers, and other identifying data without demanding any court oversight or providing any notice to the subscriber. [31] Even when courts become involved, a full consideration of the online speaker's privacy interests is far from certain. [32]

While it would be improper - and dangerous - to provide online actors a blanket of complete anonymity, [33] the routine reporting of information linking individuals to their online activity is a major privacy concern. [34] For now, much of this data collection occurs "without our awareness, much less our approval." [35] As society becomes more aware of this reporting, however, individuals may begin to censor their online conduct for fear of censure or liability, substantially undermining the right to free speech and the free exchange of ideas. [36]

This Comment explores the possibility of protecting the IP address itself as PII, [37] putting the IP address in the same category as a home [899] address, telephone number, or Social Security number and providing it and the corresponding user protection under current federal privacy law. Part II of this Comment outlines the relevant technical aspects of IP addresses [38] and the many definitions and examples of PII. [39] Part III argues that IP addresses are functionally similar to other types of PII and should be protected when in the hands of an ISP or otherwise correlated to identifying information. The argument proceeds by examining what it means for data to be "personally identifiable," [40] when IP addresses can and cannot be linked to individuals, [41] and how IP addresses are being protected at the state, federal, and international levels. [42] Finally, Part IV examines the predominate subpoena standards by which a litigant may unmask an anonymous online speaker, [43] as well as the current lack of Fourth Amendment protection for subscriber information on file with ISPs, [44] and anticipates how recognizing an IP address as PII may affect these standards and future litigation. [45]

II. Background

This Part reviews the basics of IP addresses, including some technical limitations that are later examined - and rejected - as possible barriers to identifying an individual based upon his IP address. [46] It also examines the various definitions of PII [47] and the types of data that are traditionally protected by federal law because they have the potential to identify a particular individual. [48]

A. IP Addresses and Related Technology

An IP address is a string of four numbers, each ranging from 0 to 255, [49] that serves as a unique identifier on a network to facilitate online [900] communications. [50] An IP address is tied to a computer, not its user, [51] and will normally not change when a new user logs in. [52] In this way, an IP address is analogous to a physical mailing address, which is required for the sending and receiving of postal mail. [53] However, unlike an envelope, which need not contain a return address to convey its message to the recipient, every Internet communication must contain both the sending and receiving IP addresses. [54] Because of the Internet Protocol, users communicate their return addresses to the world whether or not they know of or want this transparency. [55]

Although there are approximately four billion addresses in the current Internet Protocol, [56] many of these are reserved or unassignable, [57] and most of the useable addresses have already been assigned. [58] As a result, methods have been developed to share the limited number of remaining, viable addresses. [59] The two methods relevant here are dynamic addressing and Network Address Translation.

Critical network resources, such as servers and printers, are often given "static," or permanent, addresses so that they are easily found by other devices on the computer network. [60] Most end-user computers, however, are provided a "dynamic" address selected out of a pool and administered by an ISP. [61] An ISP may have more customers than it has assignable addresses, but dynamic addressing allows it to provide an address only to those users connected at any given time. [62] When a user disconnects, his address is put back in the pool and may [901] later be assigned to a different user. [63] Dynamic addressing allows a large number of computers to share a small number of addresses.

The current Internet Protocol is further modified by a protocol called Network Address Translation, or NAT. [64] NAT allows network administrators to assign a single public IP address to the router or modem that provides the central point of access to the Internet. [65] All of the computers and devices connected to that router are then given a local, private IP address. [66] To the internal network administrator, all of the computers retain separately identifiable IP addresses and can be tracked down with these numbers. [67] To the world, however, hundreds or even thousands of internal computers appear as a single public IP address. [68] No matter which computer accesses a Web site, the Web site will see only the address of the router. [69]

While dynamic addressing and NAT have slowed address exhaustion, the current Internet Protocol is expected to be completely assigned by 2011 or 2012. [70] As a result, the transition to the new Internet Protocol, called IPv6, [71] will soon be accelerated. Unlike current IP addresses, many IPv6 addresses will include a unique code dictated by a computer's hardware, in effect making IPv6 addresses globally unique and permanently assigned to particular devices. [72] IPv6 is unlikely to suffer from the address exhaustion that plagues the current protocol: the new system creates a 128-bit address, providing for approximately 340 undecillion - 340,000,000,000,000,000,000,000,000,000,000,000,000,000 - possible [902] addresses. [73]

Whether the address is from the current or future Internet Protocol, the take-away points are few. An IP address is assigned to a computer or other device accessing the Internet and is communicated between devices as part of the normal data exchange. [74] Some of these devices, especially those that host Web sites, record these numbers for future use. [75]

B. Defining Personally Identifiable Information

Determining what kinds of data should be protected under federal privacy law remains difficult, as there is no single definition of PII. [76] To date, Congress has rejected comprehensive privacy legislation in favor of a large collection of statutes, each of which protects specific types of information in particular circumstances. [77] The Children's Online Privacy Protection Act (COPPA), for example, regulates the online collection of information from children under the age of thirteen [78] but applies only if the Web site is directed to children or the operators have actual knowledge that their visitors are not of age. [79] The Video Privacy Protection Act of 1988 protects the disclosure of a customer's video rental records [80] but may not protect similar records collected online. [81]

These privacy statutes enumerate the data that they are enacted to protect, and these bits of information can be divided into three distinct groups. [82] The first group consists of information that is commonly [903] protected because it can identify a specific individual: names, [83] home addresses, [84] e-mail addresses, [85] telephone numbers, [86] and Social Security numbers. [87] The second group contains data that is easily combined with PII, [88] acts as PII, [89] or is central to the purpose of the enacting statute. This second group includes dates of birth, [90] photographs, [91] video rental records, [92] driver's license numbers, [93] biometric data, [94] and alien registration numbers or other unique identification numbers. [95] In the third group is aggregate data, which is a collection of data that "does not identify particular persons." [96] Aggregate data typically is not viewed as privacy-threatening and is usually excluded from protection. [97]

Some commentators believe this enumerative approach to privacy law fails to protect important pieces of private data. [98] Statutory attempts at defining PII, [99] "personal information," [100] or "means of identification," [101] however, have provided little direction in determining [904] what other types of information should be protected. [102] COPPA, for example, merely defines personal information as "individually identifiable information about an individual." [103] Likewise, the Stored Communications Privacy Act defines personal information as "information that identifies an individual." [104]

In recent years, Congress has attempted to create new definitions of PII that would specifically address online privacy concerns, [105] but the bills carrying these failed in their respective houses. [106] The Online Personal Privacy Act of 2002 would have largely followed COPPA's definition of PII [107] but would have excluded any information inferred from the data actually collected. [108] The accompanying Senate Report gave an example: if a particular user purchased a book about diabetes from an online retailer, the name, address, and other information provided to assist the delivery of that book would be PII, but the inference that the user has diabetes or a particular interest in diabetes would not be PII. [109]

The Consumer Privacy Protection Act of 2002 would have defined PII as "individually identifiable information relating to a living individual who can be identified from that information." [110] The Act would have excluded from protection any anonymous data, inferred data, or data obtained from public records. [111]

Because of the confusion in what should be protected as personal data, other entities have constructed their own definitions. The Federal Trade Commission (FTC), for example, defined "personal information" in a consent order requiring TJX Companies, the parent company of T.J. Maxx and other discount department stores, to protect [905] its customers with reasonable security measures. [112] Among the classic examples of PII identified by the FTC were a person's name, address, telephone number, and Social Security number. [113] The order went further, demanding that TJX protect its customers' e-mail addresses, other online contact information, credit or debit card numbers, and "persistent identifiers," such as a customer number held in a "cookie." [114]

While several new laws at both the federal and state level have begun to recognize the identifying power of IP addresses, most courts continue to refuse to classify them as PII. The remainder of this Comment argues that Congress should adopt - and courts should recognize - a definition of PII that incorporates and protects a user's IP address when it may be linked to that user's identifying information.

III. IP Addresses Acting as Personally Identifiable Information

This Part examines the circumstances in which an IP address should be recognized as PII. Because an IP address is similar in form to other PII and can be used to identify an individual and his online activity, it should be protected as PII when in the hands of an ISP or otherwise correlated to personal information about the user. [115] When an IP address cannot be linked to an individual, such as when it is stored by Web servers without any of the user's contact information, it should not be regarded as personal data. [116] This conclusion is supported by the apparent overall purpose of federal privacy law: to protect data only when it may be linked to a particular individual. [117]

[906]

A. PII Is Information That Has the Potential to Identify an Individual

As examined above, Congress has found it difficult to clearly define PII and the types of data that should be protected. [118] There is an inherent conflict between enumerating bright-line examples of PII and protecting data only when it identifies an individual in practice. [119] In fact, four of the most protected pieces of data need not identify a single person: multiple people may have the same name, [120] multiple residents may share the same home address and telephone number, and multiple users may log in to the same e-mail address. [121] Date of birth, which is listed as a "means of identification" under the False Identification Crime Control Act, [122] is arguably the least tied to a single individual because of the vast number of people who share the same birthday. Of the most commonly listed examples of PII, only a Social Security number appears to be completely tied to one individual. [123] In contrast, biometric data, "such as fingerprint, voice print, retina or iris image," [124] is probably the most effective type of PII due to its uniqueness but is rarely listed as PII among the statutes.

Taken together, [125] the various definitions and examples of PII suggest that what is meant by "personally identifiable information" is not a piece of data that always identifies an individual but a piece of data that could identify an individual given the totality of the circumstances. [126] [907] When aggregated, even trivial data may help identify a person, making that data collectively worthy of protection. [127]

If this is the proper definition of PII, privacy law should seek to protect any data that could identify an individual, excusing that data from protection only if it is rendered sufficiently anonymous or incapable of identifying an individual in practice. [128] Because it may be impossible to determine, ex ante, whether a particular piece of information will actually identify an individual, precautions must be taken to protect information that is likely to do so. [129] Federal privacy statutes appear to address this concern by providing protection to bits of data - such as name, phone number, and house address - that are widely considered personal even if they do not always point to a specific individual. [130]

This understanding of what it means for information to be "personally identifiable" supports a detailed examination of when IP addresses can and cannot be linked to individuals. As the following Sections explore, an IP address should not be considered personal data by itself, but it may become personally identifiable when correlated to other data about an individual.

[908]

B. By Itself, an IP Address Is Not Personal Data

An IP address cannot identify an individual by itself because it is merely a string of numbers. [131] Instead, it must be correlated to other information about the user, such as addressing logs maintained by ISPs. [132] Privacy law should not, therefore, protect IP addresses when they are not correlated to other PII, such as when they are maintained by Web site operators in normal network traffic logs.

In 2006, the Sixth Circuit Court of Appeals had an opportunity to examine whether an IP address could qualify as PII in the case *Klimas v. Comcast Cable Communications, Inc.* [133] An Internet subscriber alleged that his ISP, Comcast, violated the Cable Communications Policy Act by creating and storing a database linking each user's IP address to the Web sites he visited. [134] The subscriber claimed that Comcast had the ability to correlate this database with its addressing database linking each subscriber to his IP address and could, therefore, associate online activity with the actual identity of its subscribers. [135] The parties agreed that the dispositive issue was whether an IP address could be PII as defined in the Act. [136]

The district court first ruled that dynamic IP addresses, such as those stored in Comcast's database, are not PII because "a dynamic IP address is constantly changing.... Unless an IP address is correlated to some other information, such as Comcast's log of IP addresses assigned to its subscribers.... it does not identify any single subscriber by itself." [137] The court granted Comcast's motion to dismiss, reasoning that an IP address could not be PII as defined in the statute absent evidence of actual correlation with the subscriber information. [138]

While ultimately affirming the district court's dismissal of the case, the Sixth Circuit avoided addressing the question of PII by holding that Comcast, as a provider of broadband Internet service, was not an operator of a "cable system" as defined in the Act. [139] The court noted, however, that not all IP addresses are dynamic, and while "IP addresses do not in and of themselves" reveal a subscriber's identity, that information could be "gleaned if a list of individual subscribers is [909] matched up with a list of their individual IP addresses." [140] The court stated that the collection of data linking a subscriber's IP address to the Web sites he visited could be a proper inquiry under the Act only if this information was subsequently correlated to subscriber identities. [141] The court pointed to the Act's language that "aggregate data which does not identify particular persons" cannot be PII. [142] Without a correlation between databases, Comcast could not link its subscribers to their online conduct. [143]

While the Sixth Circuit did not have an opportunity to rule whether an IP address is PII within the definition of the Cable Communications Policy Act, the court's language makes clear that under its standard, an IP address by itself is not personally identifiable, while an IP address correlated to subscriber information could be PII.

This conclusion is fairly intuitive. [144] An IP address is only a group of four numbers between 0 and 255; the address is not intended to have any special relationship with an individual but is instead dispersed at random from a pool of available addresses maintained by the ISP. [145] Because the address may change whenever the user connects to the Internet, the use of any particular address will be measured in hours, days, or weeks but will not become permanent in most circumstances. [146] Without a correlation to other identifying information, an IP address is only a number and cannot point to the identity of an individual user. [147]

This fact does not, however, support completely excluding IP addresses from the list of personal data. As examined above, most of the data typically regarded as "personally identifiable" has no inherent connection to an individual. [148] A street address does not contain [910] the name of the person living there. Telephone numbers, Social Security numbers, and driver's license numbers are, like IP addresses, simply numerical sequences. [149] Most of the information protected by federal statute as personally identifiable must be correlated to other data in order to actually identify an individual. [150] IP addresses, therefore, are not unique in their need for correlation to other data to render them protectable PII. [151]

C. IP Addresses Are Assigned to Computers, Not People

Some courts have refused to recognize an IP address as PII because the number is assigned to a computer rather than to a particular user. The U.S. District Court for the Central District of California, in ruling on a motion to preserve and produce logs of IP addresses that had been used to download copyrighted music files, noted, "As an IP address identifies a computer, rather than a specific user of a computer, it is not clear that IP addresses ... are encompassed by the term 'personal information.'" [152] Similarly, the U.S. District Court for the Western District of Washington, faced with an allegation that Microsoft violated its own privacy policy by storing its customers' IP addresses, held that an IP address is not personally identifiable. [153] The court reasoned that, "In order ... to be personally identifiable, [information] must identify a person. But an IP address identifies a computer, and can do that only after matching the IP address to a list of a particular Internet service provider's subscribers."

[154] These decisions rely too heavily on a colloquial understanding of the words "personally identifiable" without examining the qualities of other PII. [155] It is true that an IP address is assigned to a computer, not a person. [156] This rationale is equally applicable, however, to other types of data that federal statutes nonetheless protect as PII. A house [911] address, for example, is assigned to a building, not a person. [157] A telephone number is assigned to a telephone line, not a person. [158] An e-mail address identifies an electronic mailbox stored on a computer hard drive, and a date of birth identifies a specific day in history.

These types of information may be personally identifiable in some circumstances but not in others. [159] If only one person lived at a particular house address or had access to a specific telephone, the address and telephone number would be directly linked to that person. It would be reasonable, for example, to attribute calls made from a particular cell phone number to the individual who carries the phone every day. Attributing a call to a particular individual may not be fair, however, if many people have ready access to the phone. [160]

Whether or not these pieces of data identify an individual on their own, they often can identify an individual when aggregated. [161] As one study found, combining a gender, a birthdate, and a ZIP code is enough to uniquely identify 87% of the United States population. [162] It is prudent, therefore, to provide more protection to compilations of data than that afforded individual bits of information. [163]

IP addresses present the same possibilities: they may be closely linked with a particular person and may become personally identifiable when combined with other PII. [164] When an IP address can be associated with a particular computer to which one person or a small number of persons has access, the IP address becomes more akin to [912] traditional PII. [165] Unlike other PII, the IP address can go beyond identification and actually associate a person with the content of his online activity. [166]

D. An IP Address Can Identify an Individual and His Online Activity

Three primary concerns may lead a court to question whether an IP address can constitute personally identifiable information. First, most computers use a dynamic IP address that, by definition, can change. [167] A court may ask how an IP address can be PII when it may be assigned to multiple subscribers in any given timeframe. [168] Second, the Network Address Translation protocol may operate to provide many computers with a single external IP address, restricting the ability to track online conduct to a particular computer or user. [169] Third, even if an IP address were tethered to a single computer, [170] the online conduct may have been initiated by any person who had access to that computer and might not, therefore, be fairly attributable to any individual. [171]

Courts that have faced these circumstances have had no problem utilizing IP addresses to attribute online conduct to particular persons. The following Sections examine why these technical aspects of IP addressing should not prevent the proper conclusion that IP addresses may be PII.

1. Dynamic IP Addresses Can Be Traced Back to an Individual

While most computers utilize dynamic IP addresses assigned to them by an ISP, ISPs commonly log these assignments. [172] When provided with a particular date and time of interest, an ISP can often determine to which subscriber account a particular IP address was assigned. [173] Because ISPs retain these logs for only a limited amount of time, the crucial factor in this process is the timeliness of the request [913] for identification. [174] Nevertheless, most ISPs reassign the same address to a subscriber every time he logs on to the network. [175] Even with dynamic addressing, a computer may retain a single IP address assignment for months at a time. [176] In practice, then, even dynamic IP addresses can be associated with particular individuals. [177]

In the 2010 case *United States v. Vosburgh*, [178] the Third Circuit Court of Appeals examined the process by which an ISP links an IP address back to a particular subscriber. There, an undercover FBI agent posted a dummy Web link advertising child pornography. [179] When the defendant clicked on the link, his IP address was recorded into a log file on the agent's computer. [180] In reviewing the trial testimony provided by the defendant's ISP, Comcast, the Third Circuit explained how the defendant was linked to his IP address. [181]

A witness from Comcast ... explained that Comcast can trace an IP address back to a particular customer's account, through IP assignment logs that go back 180 days. Finally, he testified that between October 20 and October 30 of 2006, IP address 69.136.100.151 was assigned to an account registered to [the defendant]. [182]

Identifying a defendant through IP addressing logs is often a crucial step in criminal cases arising from online activity. In *United States v. Stielger*, for example, an anonymous source provided a police department with evidence of child pornography originating from three dynamic IP addresses. [183] The police department notified the FBI, which issued a subpoena to the ISP that had assigned the addresses. [184] The ISP reviewed its logs, determined that all three addresses had been used by the defendant, and provided the FBI with the defendant's [914] name and home address. [185] The defendant was indicted and convicted of various child pornography charges. [186]

Identifying an online actor through ISP logs is not limited to criminal cases. In *In re Charter Communications, Inc.*, more than two hundred file-sharers were personally identified by their dynamic IP addresses. [187] The Recording Industry Association of America (RIAA) used tracking software to discover the IP addresses assigned to ninety-three Charter subscribers who were suspected of downloading and distributing copyrighted music. [188] The RIAA obtained subpoenas from the district court clerk requiring Charter to release the names, addresses, and e-mail addresses of the subscribers. [189] Charter opposed the subpoena, but its motion to quash was denied

and the district court ordered production of the information. [190] Charter subsequently released the names and addresses of 150 subscribers who had been notified of the subpoenas and another 50 to 70 who had not received notice. [191] The Eighth Circuit Court of Appeals later vacated the order, reasoning that it had been improperly issued under § 512(h) of the Digital Millennium Copyright Act. [192] The court ordered the RIAA to return the data without making any record of any further use of the subscribers' personal information. [193]

2. An IP Address Can Identify an Individual Even on a Private Network

The commonplace use of Network Address Translation may be seen as a barrier to identifying an individual with an IP address. [194] With NAT, each computer on an internal network uses a "private" IP address, while the entire network shares a "public" IP address. [195] This means that external Web servers will log the one public IP address no matter which private computer initiated the connection. However, data logs maintained in the normal course of business will often allow the private network manager to trace specific transmissions and online [915] activity to a single internal address in much the same way that an ISP traces communications on its network to a single subscriber account. [196] As a result, the NAT protocol does not prevent the identification of a user when the network manager cooperates with attempts to track down the source of online activity. [197]

The 2007 case *United States v. Heckenkamp* provides an example. [198] Qualcomm Corporation's computer administrator discovered that the company's computer systems had been accessed without authorization. [199] Through a reverse lookup procedure, the administrator determined that the hacker's public IP address had been assigned to the University of Wisconsin. [200] The administrator contacted the university's network investigator, who discovered that the hacker had utilized a computer with a private IP address ending in "117." [201] By cross-referencing the private IP address on multiple university servers, the investigator discovered that the address had recently been assigned to the defendant, an on-campus student. [202] After the investigator physically inspected the defendant's computer to confirm his findings, the FBI obtained a search warrant to seize the computer. [203] The defendant was indicted on multiple counts of recklessly causing damage through unauthorized access to a computer system in violation of federal law. [204]

3. An IP Address Can Provide Probable Cause to Suspect an Individual of Online Activity

The two preceding arguments do not represent any real limitation on the ability of an IP address to identify an individual, provided that the appropriate addressing logs are available. The third concern, however, is not easily dismissed: there may, in fact, be no way to definitively link a particular person with the online conduct emanating from a particular computer or IP address. [205] A user may, for example, access online content without ever providing identifying credentials. [206] If many people use a single computer, it would be difficult to attribute [916] online conduct to any one of them based solely on that computer's IP address. [207]

This dilemma may be avoided by requiring some authentication at the computer terminal. [208] When a user signs in to a personal account by entering a username and password, the authentication process is logged by either the local computer or the network servers. [209] By cross-referencing the IP logs with the user authentication logs, a network administrator can identify what user account was signed in at the time of some questionable online activity. [210] Absent photographs or video of the person sitting at the computer at the time in question, a user authentication log is likely to provide the strongest evidence of who actually accessed the online material.

Even without an authentication log, however, the link between an IP address and the Internet subscriber may provide enough circumstantial evidence to suspect a particular individual of some litigious or criminal online activity. [211] Since 2000, the Third, Fifth, Sixth, Eighth, Ninth, and Tenth Circuit Courts of Appeals have all held that a search warrant is supported by probable cause when it uses an IP address and an ISP logging database to identify a defendant. [212]

In the 2007 case *United States v. Perez*, [213] for example, the FBI subpoenaed an ISP to obtain the name and home address of a subscriber whose IP address had recently been used to post child pornography. [214] Upon executing a search warrant on the subscriber's address, the FBI discovered that three people resided in the house, each maintaining a separate "occupancy unit." [215] The defendant argued that the occupancy by two other persons and the wires running into each bedroom [917] should have alerted the officers to the possibility that one of the other housemates had been responsible for the online conduct. [216] On appeal, however, the Fifth Circuit held that the officers had probable cause to search the defendant's premises; reasoning that the Internet account had been registered in the defendant's name, which created a "fair probability" that the defendant was responsible for the online conduct. [217] The court noted that, although "it was possible that the transmissions originated outside of the residence to which the IP address was assigned, it remained likely that the source of the transmissions was inside that residence." [218]

In *United States v. Kennedy*, [219] the FBI obtained a court order directing disclosure of the subscriber information related to an IP address assigned to a computer allegedly containing child pornography. [220] The Internet account was registered in a woman's name but also listed an e-mail address for a man. [221] Upon questioning the man, the FBI determined that he was the primary user of the Internet service. [222] This admission, along with other supporting facts obtained during the questioning, [223] provided probable cause to search the defendant. [224]

As the above cases demonstrate, an Internet user can often be identified by the IP address assigned to his computer despite the alleged technical barriers. [225] An IP address, then, must be PII when in the hands of an ISP or another entity that can make the correlation between the address and the individual. [226] The reservations that some courts have about recognizing an IP address as PII likely stem from the fact that only an ISP can consistently correlate an IP address to a subscriber account. [227] When the IP address is collected by entities [918] other than the ISP, the address must be specifically correlated with other personal data in order to identify an individual user. [228] If Web sites do not collect other PII, or do not correlate other PII to IP addresses, the Web site owners cannot trace the IP address back to an individual. [229] Regulating the use of IP addresses by these entities would restrict their legitimate business operations without providing a significant counterbalancing benefit to user privacy.

This is a clear distinction, and one that may be used to establish legal rules protecting a user's IP address only when it may act as personal data. In addition, rules protecting IP addresses only when they are in the hands of an ISP or are correlated to other PII would fit within the federal framework of privacy law, which protects data only when the specific circumstances threaten individual privacy. [230]

E. The Movement to Protect IP Addresses

Despite the skepticism, there is a growing movement recognizing the identifying power of IP addresses. For one, a number of states have adopted definitions of PII affording protection to IP address information and the individual behind the computer. [231] In Indiana, for example, a criminal procedure law protects information that identifies a victim of domestic violence, dating violence, sexual assault, or stalking. [232] The list of protected information includes the victim's name, address, telephone number, and IP address. [233] Likewise, a Connecticut law lists IP addresses among the "basic subscriber information" that may be obtained during a criminal investigation of a registered sex-offender only upon judicial order. [234]

Minnesota's "Internet Privacy" statute is the first state law to explicitly regulate an ISP's disclosure of its subscribers' personal information and browsing habits. [235] The statute defines PII to include any [919] information that (1) identifies a subscriber by "physical or electronic address or telephone number"; (2) discloses the subscriber's Web site visits or requested materials; or (3) contains any of the contents of the subscriber's data-storage devices. [236] ISPs are prohibited from releasing this information except in limited circumstances. [237] However, because those circumstances include the issuance of a standard subpoena, warrant, or court order, [238] the actual level of protection afforded will continue to depend upon courts' willingness to allow the identification of online speakers.

The new federal Health Insurance Portability and Accountability Act (HIPAA) privacy rule explicitly protects IP addresses. [239] The regulation allows health providers to

release patient information only after it is scrubbed of all "individually identifiable ... information." [240] Data that must be removed includes most of the commonly recognized forms of PII, including telephone numbers, Social Security numbers, and biometric data. [241] The regulation adds IP addresses to this list. [242]

In July of 2010, U.S. Representative Bobby Rush introduced an online privacy bill to the House Committee on Energy and Commerce that would protect IP address information when it is used to build an online profile for behavioral advertising. [243] In addition to traditional forms of PII, the Best Practices Act would protect

any unique persistent identifier, such as a customer number, unique pseudonym or user alias, IP address, or other unique identifier, where such identifier is used to collect, store or identify information about a specific individual or to create or maintain a preference profile. [244]

[920] The Act, which builds upon a May 2010 proposal drafted by U.S. Representatives Rick Boucher and Cliff Stearns, [245] would require any "covered entity" [246] that collects such information to provide notice of collection practices and provide users an opportunity to opt out of data collection. [247] Disclosure of the protected information to third parties would require the individual's express consent, [248] except in cases of prior consent, fraud detection, imminent danger, publicly available information, or compliance with law - such as a statute, subpoena, or summons. [249]

Notably, the Act would not require covered entities to allow users to opt out when data collection is required for an "operational purpose." [250] This exception would likely allow ISPs and Web site operators to continue to use and maintain IP address information necessary to deliver Internet services. [251] Consistent with the position taken in this Comment, the exception implicitly recognizes that IP addresses are necessary for the operation of Internet services and should only be protected as personal data when correlated to other identifying information. [252]

Abroad, the European Union Data Protection Working Party found in 2008 that IP addresses should be protected as "personal data." [253] As the Working Party concluded,

An individual's search history is personal data if the individual to which it relates, is identifiable. Though IP addresses in most cases are not directly identifiable by search engines, identification can be achieved by a third party. Internet access providers hold IP address [921] data. Law enforcement and national security authorities can gain access to these data and in some Member States private parties have gained access also through civil litigation. Thus, in most cases - including cases with dynamic IP address allocation - the necessary data will be available to identify the user(s) of the IP address. [254]

The Working Party went beyond regulation of ISPs, imposing limitations on Web site operators who use and maintain IP address information whenever the addresses are correlated with other personal information. [255]

The High Court of Ireland reached an opinion consistent with the position proposed in this Comment in its 2010 decision, *EMI Records Limited v. Eircom Limited*. [256] EMI and other copyright owners sued Eircom, an ISP, for the peer-to-peer file sharing of copyrighted material conducted on Eircom's network. [257] The parties settled, developing a protocol by which EMI would inform Eircom of the IP addresses used to download its copyrighted material, and Eircom would warn, and possibly disconnect service to, the associated subscribers. [258] In examining the lawfulness of the settlement terms, the High Court asked whether IP addresses, in the hands of EMI and its agents, constituted "personal data" under the Data Protection Act. [259] Unlike the laws of the United States, the Act provided significant direction by defining personal data as "data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller." [260]

Examining the specifics of the settlement protocol, the High Court concluded that IP addresses in the hands of EMI or its agents could not qualify as personal data. [261] The court reasoned that:

none of the plaintiffs have any interest in personally identifying any living person who is infringing their copyright by means of the settlement and protocol... There seems no legal avenue open to them to get that information apart from an application for the names and addresses of the copyright thieves to the internet service provider. [262]

[922] This conclusion is consistent with the above argument that an IP address is personally identifiable only when correlated to other personal data, such as when in the hands of an ISP. During execution of the settlement protocol, EMI would know only the IP address of a user suspected of copyright infringement and would have no means by which to link that information to particular persons. [263] The court correctly concluded that IP addresses should not be protected as personal data in such circumstances. The court did not, however, have occasion to question whether the IP address information should be protected when in the hands of Eircom itself.

The next Part examines the possible practical results of this movement to classify IP addresses as PII. It examines how IP addresses could be incorporated into the federal statutory framework, [264] how doing so may affect the current subpoena standards by which a private litigant may unmask an anonymous online speaker, [265] and how online actors' expectations of privacy in online communications may be affected. [266]

IV. Impact

Both the feasibility and the effect of incorporating protections for IP addresses into current privacy law would depend upon the statutory scheme at issue. [267] Some statutes provide a catch-all clause allowing courts to afford protections to unspecified - but nonetheless private - information. [268] If an IP address falls within these catch-all clauses because it can identify a particular person, then the release of such an IP address and the associated subscriber information held by an ISP would be subject to the particular statute's subpoena standards.

Other statutes, however, leave no room for new types of PII or do not set specific standards by which a litigant can subpoena the release of the information protected. In cases brought under those statutes, courts must balance the litigants' competing interests in the production of the information. When IP address information is at issue, courts would be better able to balance these interests if they explicitly [923] recognized the personal nature of the IP address and its ability to link an individual to his online conduct.

In addition, classifying IP addresses as PII would support reexamining Fourth Amendment law as applied to basic subscriber information. [269] Current law holds that, under the third party doctrine, Internet subscribers do not have a reasonable expectation of privacy in this information because they have voluntarily exposed it to their ISPs. [270] Protecting an IP address as personal information, however, would support providing stronger protections to the data linking online content to particular subscribers, especially when Internet users must release this information in order to obtain Internet service. [271]

The following Sections briefly examine the myriad of subpoena standards applicable when unmasking online speakers [272] and the current Fourth Amendment law as applied to basic subscriber information before imagining how these may change when IP addresses are considered personal information.

A. Subpoena Standards for Unmasking Online Defendants

The thin veil of anonymity that the Internet provides often requires that a litigant seeking redress from actions conducted online initially file his complaint against an unnamed party, the Doe defendant. [273] The plaintiff will then seek a subpoena or court order requiring the appropriate third party to expose the Doe defendant's true identity. [274] The statute providing protection to the personal information at issue may stipulate the appropriate subpoena standard. [275] If the plaintiff obtains a subpoena pursuant to a statutory provision, the Doe defendant may not have a viable method by which to avoid his identification. [276]

Some statutory standards strongly favor the plaintiff's interest in identifying a defendant. The Digital Millennium Copyright Act (DMCA), for example, expressly allows copyright owners to subpoena [924] ISPs for the identification of alleged infringers. [277] If the plaintiff submits a subpoena request having the required form and content, the district court clerk is instructed to "expeditiously issue" the subpoena. [278] The ISP, upon its receipt of the subpoena, must "expeditiously disclose" the information requested. [279] While the circumstances in which the DMCA authorizes disclosure are limited, [280] exposing a Doe defendant can be fairly automatic and quickly accomplished under the DMCA standard.

Other statutes provide more protection to the defendant's personal information. The Video Privacy Protection Act, for example, requires that a party seeking a court order to expose video rental records make a showing of "compelling need" and provide the consumer with reasonable notice and an opportunity to contest the disclosure. [281] The plaintiff may obtain an individual's name and address only if that person is given an opportunity to prevent the disclosure. [282] Likewise, the Cable Communications Policy Act requires that an individual be notified of a court order authorizing the disclosure of his PI to a private entity. [283] If the information is to be disclosed to a government entity, there must be clear and convincing evidence that the individual is suspected of a crime and that the information sought will be material to the case; the individual must also be given the opportunity to appear and contest the claim. [284]

Finally, some statutes provide strong protections to individuals in only limited circumstances. The Stored Communications Act, for example, requires a warrant or court order before a stored electronic communication or PI is released to a government entity. [285] A court order is obtainable only upon specific and articulable facts supporting a reasonable belief that the information is relevant and material to an ongoing criminal investigation. [286] Because the Act is concerned only with governmental invasions of privacy, however, it provides no protection when a private entity seeks the release of customer records; the statute explicitly authorizes the release of customer records or [925] other information to "any person other than a governmental entity." [287]

Absent statutory direction, courts must weigh the parties' competing interests: the plaintiff's interest in seeking redress for alleged harms and the defendant's interest in remaining anonymous. [288] Setting the subpoena standard too high might leave the plaintiff without an opportunity to proceed upon even a valid claim, [289] while setting the standard too low will fail to provide defendants with adequate privacy protection and might allow their identities to be exposed without adequate notice. [290] More importantly, a standard set too low could allow the plaintiff to use the legal process to unmask an online actor merely to later seek extra-judicial retribution. [291]

Many courts have recently addressed this balancing act in the context of defamation actions. [292] The defamation claim is particularly interesting because it already requires balancing the speaker's right in free speech against the subject's interest in redressing harms to his reputation. [293] In the online world, the relevant factors may tip in the plaintiff's favor: the Internet allows speakers to reach more people at a faster rate, [294] potentially multiplying the effects of defamatory speech, [295] and the underlying technology provides a method by which [926] the speaker may be easily identified. [296] Courts have, therefore, grappled with setting a standard that appropriately protects online speakers.

Three distinct standards have emerged from the case law. [297] Providing the least protection to a speaker's anonymity is the "good faith" standard articulated by a Virginia trial court in *In re Subpoena Duces Tecum to America Online*. [298] In that case, an anonymous publicly traded company sought to expose the identities of five John Doe defendants who had allegedly made defamatory comments in an America Online chatroom. [299] Although recognizing the Does' right to anonymous free speech on the Internet, [300] the court found in favor of the compelling state interest in protecting companies from actionable communication. [301] The court held that it may order an ISP to disclose the identity of a subscriber when the plaintiff's pleadings or evidence show a "legitimate, good faith basis" to claim that it was the victim of actionable conduct and the identity of the subpoenaed party is "centrally needed to advance that claim." [302] This standard is fairly deferential to the plaintiff's interest in seeking redress for alleged harms. [303]

At the other end of the spectrum is the "summary judgment" standard established by the Supreme Court of Delaware in *Doe v. Cahill*. [304] A public official sought to expose the identity of an online poster who allegedly made defamatory remarks on a newspaper blog lambasting the official's "failed leadership" and "character flaws." [305] The trial court adopted the "good faith" standard and held that the official could subpoena the speaker's ISP for his identifying information. [306] On Doe's interlocutory appeal, the state supreme court expressed concern that setting the subpoena standard too low may cause online actors to self-censor out of fear of future liability. [307] A "sue first, ask questions later" approach and a minimally protective subpoena standard could act to "discourage debate on important issues of [927] public concern." [308] Finding the good faith standard too easily met, the court adopted a stricter "summary judgment" standard. [309] Under this standard, a plaintiff seeking to expose an anonymous defendant must provide prima facie evidence of his claim and make reasonable efforts to notify the defendant of a subpoena or application for court order. [310] Because the plaintiff would have easy access to proof of most of the elements of the claim, the court said, it would not be overly burdensome to require prima facie proof before disclosing the defendant's identity. [311]

The U.S. Court of Appeals for the District of Columbia Circuit recently adopted a standard very near the Cahill summary judgment standard. [312] In *Solers, Inc. v. Doe*, a Virginia corporation subpoenaed a trade association for the identifying information of a tipster who had falsely alleged that the corporation violated copyright law by using unlicensed software. [313] Unlike other defamation cases, the Doe defendant had not posted his accusation on an Internet message board but had rather sent a personal message using the trade association's Web site. [314] Despite this factual difference, and the recognition that a trial court may need to modify the test "depending on the type of injury alleged," [315] the court adopted a summary judgment standard. [316] The Solers test required that the plaintiff (1) adequately plead the elements of his claim and offer evidence creating a genuine issue of material fact on every element within his control; (2) use reasonable efforts to notify the defendant of the subpoena; (3) show that the information sought would enable the plaintiff to proceed with his lawsuit; [317] and (4) delay further action to allow the defendant a reasonable time to move to quash the subpoena. [318]

[928] Between the stringent "summary judgment" standard and the deferential "good faith" standard lies the standard established by the U.S. District Court for the Northern District of California in *Columbia Insurance Co. v. Seescandy.com*. [319] A trademark owner sought to identify the party who started a Web site using the owner's registered trademark. [320] The court held that a "motion to dismiss" standard sufficiently balanced the parties' competing interests. [321] By requiring the plaintiff to plead an actionable claim and a likelihood that the discovery would reveal the identity of the Doe defendant, the standard would help "to prevent abuse of this extraordinary application of the discovery process." [322]

While these subpoena standards are quite varied, there are certain elements consistent within each. [323] Before unmasking a Doe defendant, most courts require a plaintiff to provide adequate notice to the defendant, to make some evidentiary showing of the merits of his claim, and to explain why the need to expose the online actor's identity outweighs that person's First Amendment right to anonymous speech. [324]

B. The Fourth Amendment Provides No Protection to Transactional Information

Although an in-depth discussion of Fourth Amendment jurisprudence as applied to the Internet is outside the scope of this Comment, [325] one critical concern must be mentioned in light of the many criminal cases discussed above. A criminal defendant may be tempted to argue that he has an objectively reasonable expectation of privacy in the subscriber information on file with his ISP. [326] The defendant may reason that he disclosed his name, address, browsing history, and other personal information to his ISP only for the limited purpose of [929] obtaining Internet services and did not consent to the release of that information to third parties. [327]

This argument, however, would probably be unavailing. "Every federal court to address this issue has held that subscriber information provided to an Internet provider is not protected by the Fourth Amendment's privacy expectation." [328] Under the third party doctrine, all objectively reasonable expectations of privacy are extinguished when users voluntarily expose data to third parties. [329] Because Internet users "voluntarily convey[] all this information to [their] Internet and phone companies [they] assume[] the risk that those companies [will] reveal the information to the police." [330]

This result is generally in accordance with similar case law governing the disclosure of information voluntarily exposed to telephone operators and similar entities. [331] The apparent unwillingness to distinguish between older technology and the Internet is understandable. [332] As the Supreme Court recently noted in a case examining whether a government employee had a reasonable expectation of privacy in the text messages sent from his employer-issued pager, "The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear." [333]

Nevertheless, it may be time to reexamine Fourth Amendment law, particularly the third party doctrine, as applied to the Internet. [334] In his famous dissent to the 1929 wire-tapping case *Olmstead v. United States*, [335] Justice Louis Brandeis expressed concern that "ways may some day be developed, by which the Government, without removing [930] papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home." [336] Today, with the help of ISPs, the government has easy access to these "papers." IP addresses allow the "government [to] learn the names of stores at which a person shops, the political organizations a person finds interesting, a person's sexual fetishes and fantasies, her health concerns, and so on," [337] but Internet users currently have no reasonable expectation of privacy in the subscriber data linking this information back to them as individuals. To say that Internet subscribers voluntarily exposed this information to ISPs is simplistic and misleading. After all, the only way to avoid releasing this information to an ISP is to not use the Internet at all. [338]

Interestingly, New Jersey constitutional law may provide a model for updating the third party doctrine. In the 2008 case *State v. Reid*, [339] the Supreme Court of New Jersey held that the state's constitution affords its citizens a reasonable expectation of privacy in the subscriber information provided to ISPs. [340] The defendant Shirley Reid was indicted for second-degree computer theft after she allegedly logged onto a Web site belonging to one of her employer's suppliers, changed her employer's password to the site, and altered the employer's shipping address. [341] The supplier subsequently informed Reid's employer of the changes and provided it with the IP address that the perpetrator had used to log onto the Web site. [342] The employer issued a municipal subpoena to the associated ISP and received Reid's name, home address, telephone number, account number, e-mail address, and method of payment in return. [343]

The trial court granted Reid's motion to suppress the subpoena evidence and the appellate court affirmed, finding various procedural flaws in the subpoena and concluding that Reid had a protected privacy interest in her subscriber information. [344] On appeal, the state supreme court began by recognizing that the New Jersey constitution affords greater protection against unreasonable searches and seizures [931] than that provided by the Fourth Amendment. [345] The court reviewed *State v. Hunt*, [346] a 1982 case in which the court had extended privacy protection to telephone records by reasoning that such information was released only as a necessity for obtaining phone service. [347] Analogizing ISP records to those maintained by phone companies and banks, the Reid court reasoned that Internet users should not lose their privacy interest in information that they must release in order to obtain Internet service. [348]

In the world of the Internet, the nature of the technology requires individuals to obtain an IP address to access the Web. Users make disclosures to ISPs for the limited goal of using that technology and not to promote the release of personal information to others. Under our precedents, users are entitled to expect confidentiality under these circumstances. [349]

While adopting a viewpoint closer to that expressed in Reid would require significant retooling of Fourth Amendment jurisprudence, such changes may be necessary. As Orin Kerr, professor at George Washington University Law School, recently concluded, "The application of the Fourth Amendment to computer networks will require considerable rethinking of preexisting law" [350]

C. Recognizing IP Addresses as PII Will Help Protect Online Identity

Unsurprisingly, the burden of incorporating IP addresses into the wide and varied framework of privacy law would itself be widely different depending upon the context. Some statutes anticipate the addition of categories of data to the list of PII. COPPA, for example, lists under its definition of personal information "any other identifier that the Commission determines permits the physical or online contacting of a specific individual." [351] The False Identification Crime Control Act includes a "unique electronic identification number, address, or routing code" as a means of identification. [352] For these and similar statutes, no change need be made other than an explicit recognition that an IP address may be personally identifiable and otherwise meets the criteria of data worth protecting.

[932] Other statutes would require substantial amendment. The Stored Communications Act, for example, allows "basic subscriber information," [353] including "any temporarily assigned network address," to be obtained with a mere subpoena. [354] To protect the user's online identity as exposed by an IP address, this category of easily accessible information could be removed. Such an amendment could be in accordance with the Act's purpose: to protect the content of stored e-mail. [355] Limiting access to a user's IP address would likewise prevent the easy correlation of an individual to the content of his online activity. [356]

Once protected by statute, the IP address would be subject to the applicable subpoena standards. As discussed above, these standards would provide varying degrees of protection to the online speaker's identity. [357] This may be a desirable result. The statutes were enacted for particular purposes [358] and already strike a balance between the plaintiff's and defendant's interests. The DMCA, for example, allows subpoenas to "expeditiously issue" in order to protect the rights of copyright owners. [359] The standard weighs in favor of the plaintiff copyright owner who desires to quickly stop the distribution of his intellectual property. The Video Privacy Protection Act, on the other hand, requires a higher showing of compelling need and ample notification to the subject. [360] This balance suggests that the release of video rental records is less important to the plaintiff, less time-sensitive, and more private.

Specifically recognizing IP addresses as PII should not alter these balances. Providing due respect for the power of an IP address to identify an individual would, however, provide a better guide for courts' analyses and could alter the outcome of close cases. The 2008 case *Viacom v. YouTube* [361] presents a pertinent example. Viacom and other copyright owners sued YouTube on direct, vicarious, and contributory infringement theories for allowing users to upload and [933] view their copyrighted videos on the YouTube Web site. [362] During discovery, Viacom sought YouTube's logging database, which linked User IDs and IP addresses to the videos that each user had viewed or uploaded. [363] YouTube sought the protection of the Video Privacy Protection Act, arguing that releasing the data would allow Viacom to determine the viewing and uploading habits of individual users. [364] The district court refused to apply the Act, reasoning that YouTube's privacy concerns were speculative because the IDs and IP addresses could not in themselves identify individuals. [365] The court subsequently granted production of the database. [366]

Given the ability of IP addresses to identify users, YouTube's argument should have been given greater weight. Armed with YouTube's database, Viacom could, for example, choose the top one hundred IP addresses used to upload its copyrighted material. Viacom could obtain the names, addresses, and other personal information of the users tied to those IP addresses by issuing subpoenas to the appropriate ISPs. The company could then sue those users directly for copyright infringement in the same way that the RIAA has sued individual file-sharers. [367] While YouTube activity should probably not be hidden behind the Video Privacy Protection Act, which exists to protect the records of legitimate video rentals, the court's analysis would have been better served by recognizing that the logging database would allow Viacom to identify particular YouTube users and their viewing habits. Giving Viacom access to such a database is not a trivial matter, and it deserved the court's considered analysis of whether Viacom's interest in tracking down copyright infringers outweighed the privacy interests of potentially millions of users who would be linked to the content they had viewed on the Web site. [368]

Recognizing the ability of an IP address to identify an individual will also be important for a court's analysis when it must balance the parties' competing interests absent a statutory subpoena standard. In some circumstances, more may be at stake than merely identifying the defendant: whenever a plaintiff compels the production of logs that [934] identify IP traffic, users may be associated with the content of their online activity. [369]

Adequately protecting the online actor's interest requires that one of the more stringent subpoena standards be applied. [370] The Solers test, which requires the plaintiff

to meet the summary judgment standard and use reasonable efforts to provide notice to the defendant, [371.1] would ensure that the plaintiff's interest in exposing the defendant outweighs the defendant's interest in remaining anonymous. By requiring a plaintiff to make a significant showing of his case, a court would deter the misuse of the discovery process to expose online actors merely for extra-judicial retribution or speech suppression. [372.1] Providing the defendant notice of the subpoena and sufficient time to submit a motion to quash would ensure that a defendant with important privacy concerns is afforded an opportunity to protect his interests. [373.1]

Finally, recognizing the reality of what an IP address can do would support reexamining the application of Fourth Amendment law to these situations. Cases that hold users have no Fourth Amendment interest in the information voluntarily exposed to ISPs have viewed IP addresses as transactional data, similar to a listing of the telephone numbers a particular user dialed. [374.1] As this Comment has discussed, however, IP addresses are more likely to disclose the content of a user's online activity. Although redialing a phone number may not reveal the content of the user's previous conversation, [375.1] browsing for the particular IP address may reveal that the user visited a socially unpopular Web site or even one that contained criminalized material. This possibility means that, in some circumstances, IP addresses are more akin to the content of communications than they are transactional data and should be protected appropriately.

Whatever the context, courts should recognize the value and importance of IP addresses to online conduct and the litigation that arises [935] out of that activity. An IP address may be no more than a number, but it may be associated with a particular individual in the same manner as a home address or telephone number, pieces of data that are consistently protected as personal. In fact, IP addresses go further by linking users to their online activities. As the technology progresses, the likelihood of identifying a user will increase: with the new IPv6 protocol, most devices connected to the Internet will have a unique, static address that can distinguish that device anywhere in the world. [376.1] The technical hurdles will be removed, and all online activity will be linked to particular laptops, computers, cell phones, PDAs, and their users. [377.1]

Recognizing an IP address as personal data should not create a blanket of anonymity online. Crimes and civil wrongs are committed online every day, and those harmed by these actions deserve the appropriate remedies. Nevertheless, courts need to be able to factor online privacy concerns into their balancing of litigants' interests. The first step in improving that balancing analysis is recognizing that IP addresses can often be traced back to online actors and should, therefore, be considered personally identifiable information.

V. Conclusion

In mid-2003, the RIAA obtained seventy-five subpoenas every day, each using an IP address to unmask the identity of an alleged downloader of illegal music files. [378.1] Many such subpoenas are issued as a matter of course, [379.1] and while some courts have expressed concern for the anonymous online speaker, others have uniformly granted subpoenas without judicial oversight. [380.1] Often, the speaker's privacy concerns are never addressed. [381.1]

When courts do examine privacy interests, however, they often struggle to find the proper balance between a defendant's right to remain anonymous and a plaintiff's right to due process of law. [382.1] This struggle demonstrates the importance of IP addresses: armed with an IP address, a cooperating ISP, and an IP address log, any litigant can determine the identity of an online speaker. Like a Social Security number, home address, or telephone number, an IP address is often [936] correlated to the identifying information of a particular individual. Although the personal information on file with an ISP may not always be the actual speaker's name, identifying the Internet subscriber will usually be enough to narrow the search to a small number of individuals, such as members of a particular household. [383.1]

Despite some technical shortcomings, the IP address is more often than not able to expose the person behind the computer. As the technology progresses, IP addresses will be even more consistently tied to individual devices and their users. If courts are willing to permit this correlation to provide probable cause to suspect an individual of online activity, or to serve as circumstantial evidence tending to prove a defendant's liability for online conduct, they should also be willing to consider the privacy interests involved. Protecting IP addresses as personally identifiable information will assist courts in properly considering these interests and in balancing the litigants' expectations of online privacy.

DePaul Law Review

Copyright (c) 2011 DePaul University

DePaul Law Review

Footnotes

[1] See Matthew Sag, Copyright and Copy-Reliant Technology, 103 *Harv. U.L. Rev.* 1602, 1607 n.1 (2009) (defining the Internet age from 1994 to present).

[2] See *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334, 357 (1995) (striking down an Ohio statute banning the distribution of anonymous handbills). The importance of anonymous speech has long been recognized, chiefly in the political context. See *Talley v. California*, 362 U.S. 60, 64 (1960) ("Anonymous pamphlets, leaflets, brochures and even books have played an important role in the progress of mankind. Persecuted groups and sects from time to time throughout history have been able to criticize oppressive practices and laws either anonymously or not at all.").

[3] *McIntyre*, 514 U.S. at 357.

[4] See *Reno v. ACLU*, 521 U.S. 844, 870 (1997).

[5] As one scholar wrote, "The Internet promises to eliminate structural and financial barriers to meaningful public discourse, thereby making public discourse more democratic and inclusive, less subject to the control of powerful speakers, and, at least potentially, richer and more nuanced." Lyrrisa Barnett Lidsky, *Silencing John Doe: Defamation & Discourse in Cyberspace*, 49 *Duke L.J.* 855, 896 (2000).

[6] See *Reno*, 521 U.S. at 870; *Doe v. Cahill*, 854 A.2d 451, 456 (Del. 2005) ("Anonymous Internet speech in blogs or chat rooms in some instances can become the modern equivalent of political pamphleteering.").

[7] See *Cahill v. Doe*, 879 A.2d 943, 951 (Del. Super. Ct. 2005) (noting that the Internet "presents the real danger that users might abuse the medium by rapidly spreading defamatory information"), rev'd, 884 A.2d 451 (Del. 2005). Nevertheless, courts typically afford "greater weight to the value of free speech than to the dangers of its misuse." *McIntyre*, 514 U.S. at 357.

[8] Indeed, "the advent of the computer means ... we have the ability to be more intrusive than ever before." S. Rep. No. 100-599, at 6 (1988). See also *infra* notes 325-50 and accompanying text.

- [97] See Daniel J. Solove, Digital Dossiers and the Dissipation of Fourth Amendment Privacy, 75 S. Cal. L. Rev. 1093, 1092 (2002) (noting that the Internet "gives many individuals a false sense of privacy"). This behind-the-scenes monitoring is arguably more dangerous than even the feared telescreen of George Orwell's dystopian *Nineteen Eighty-Four*; at least there, the subjects knew of their surveillance. See George Orwell, *Nineteen Eighty-Four*, at 3 (*Signet Classics* 1950) (1949) ("You had to live - did live, from habit that became instinct - in the assumption that every sound you made was overheard, and, except in darkness, every movement scrutinized."); see also Shawn C. Helms, *Translating Privacy Values with Technology*, 7 B.U. L. Sci. & Tech. L. 288, 291-92 (2001) (comparing Internet surveillance to Jeremy Bentham's Panopticon).
- [107] Jerry Berman & Deirdre Mulligan, *Privacy in the Digital Age: Work in Progress*, 23 *Novae*, Rev. 549, 554 (1999) (noting the necessity of IP addresses for network functionality).
- [117] *United States v. Steiner*, 318 F.3d 1039, 1042 (11th Cir. 2003).
- [127] *Id.*
- [137] See *State v. Reid*, 194 A.2d 26, 33 (N.J. 2008) ("With a complete listing of IP addresses, one can track a person's Internet usage."); Berman & Mulligan, *supra* note 10, at 558; Solove, *supra* note 9, at 1145.
- [147] See Oscar H. Gandy, Jr., *Exploring Identity and Identification in Cyberspace*, 14 *Notre Dame J.L. Ethics & Pub. Pol'y* 1085, 1093 (2000).
- [157] Short for weblog, a blog is a Web site to which users post comments, hyperlinks, and other general discussion. Blog, Merriam Webster Online, <http://www.merriam-webster.com/dictionary/Blog> (last visited Jan. 14, 2011). Blogs have been at the forefront of the Web 2.0 movement in which online users become active participants rather than passive consumers of online material. See generally Tim O'Reilly, *What Is Web 2.0: Design Patterns and Business Models for the Next Generation of Software*, O'Reilly.com (Sept. 30, 2005), <http://oreilly.com/pub/a/web2/archive/what-is-web-20.html?page=3>. Blogs can reveal a wealth of private information and are, therefore, a tremendous privacy concern.
- [167] See, e.g., *Doe v. Cahill*, 884 A.2d 451, 454 (Del. 2005) (involving a blog operator who maintained a log of commentators' IP addresses).
- [177] See, e.g., *Gonzales v. Google, Inc.*, 234 F.R.D. 674, 687 (N.D. Cal. 2006) (expressing concern for the privacy of searches for sexually explicit material).
- [187] See *Id.* (noting that the government may be forced to investigate such a query); see also Omer Tene, *What Google Knows: Privacy and Internet Search Engines*, 2008 *Utah L. Rev.* 1433, 1442 ("Google records all search queries linked to a specific Internet Protocol (IP) address.").
- [197] See Gandy, *supra* note 14, at 1093; Helms, *supra* note 9, at 296.
- [207] See Paul Ohm, *The Rise and Fall of Invasive ISP Surveillance*, 2009 *U. Ill. L. Rev.* 1417, 1420.
- [217] *United States v. Steiner*, 318 F.3d 1039, 1042 (11th Cir. 2003); see also *In re Charter Commc'ns, Inc.*, 393 F.3d 771, 774 (8th Cir. 2005) (noting that only an ISP can link an IP to an individual).
- [227] See Solove, *supra* note 9, at 1143 (stating that the ISP "holds the key" to user anonymity); see also *Cahill v. Doe*, 879 A.2d 943, 955 (Del. Super. Ct. 2005) ("The ISP can readily provide the identity of its subscriber(s). But this does not mean in all instances that it should be compelled to do so."); *rev'd*, 884 A.2d 451 (Del. 2005).
- [237] Because ISPs also have the ability to record what Web sites their subscribers visit, such comparison may not be necessary in all circumstances. Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 *Stro. L. Rev.* 1193, 1233 (1998). If the ISP chooses to maintain IP address logs, it can link a user to his traffic without the aid of the Web site operators or other data aggregators. See, e.g., *Klimes v. Comcast Cable Commc'ns, Inc.*, 455 F.3d 271, 273 (6th Cir. 2006) (involving an ISP that temporarily stored data listing its subscribers' Web site visits).
- [247] If multiple users access the Internet via the same subscriber account, the IP address will likely identify all of their Internet traffic and will not, therefore, be perfectly linked to any individual user. Frederick Lah, *Are IP Addresses "Personally Identifiable Information"?*, 4 *I/S J. L. & Pol'y for the Info. Soc'y* 681, 700-01 (2008). There may be enough of a link, however, to provide probable cause for a criminal investigation of the account owner. See *infra* notes 205-24 and accompanying text.
- [257] See Helms, *supra* note 9, at 296.
- [267] Ohm, *supra* note 20, at 1420.
- [277] See Tene, *supra* note 18, at 1450 ("Search-query logs ... become privacy threatening if they can be traced back to a specific user.").
- [287] See Paige Norian, *The Struggle to Keep Personal Data Personal: Attempts to Reform Online Privacy and How Congress Should Respond*, 52 *Cath. U. L. Rev.* 893, 811 (2003) (noting that the "patchwork" nature of federal privacy law left "significant gaps in online privacy").
- [297] Shaun B. Spencer, *CyberSLAPP Suits and John Doe Subpoenas: Balancing Anonymity and Accountability in Cyberspace*, 19 *J. Marshall J. Computer & Info. L.* 493, 493 (2000); see, e.g., *State v. Reid*, 945 A.2d 26, 29 (N.J. 2008).
- [307] See James X. Dempsey, *Digital Search & Seizure: Standards for Government Access to Communications and Associated Data*, in 2 *Tenth Annual Institute on Privacy Data Security* L. 687, 703 (2009).
- [317] See Spencer, *supra* note 29, at 493; see also Dempsey, *supra* note 30, at 718 ("If the government obtains from the search engine the IP addresses associated with particular queries, it can compel ISPs to identify those individuals.").

[32] See Matthew Mazzotta, Note, *Balancing Act: Finding Consensus on Standards for Unmasking Anonymous Internet Speakers*, 51 B.C.L. Rev. 833, 855-58 (2010) (examining the emerging discovery standards for unmasking online speakers and noting that "only one standard in the survey requires a court to consider the anonymous speaker's expectation of privacy").

[33] See *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334, 357 (1995) ("The right to remain anonymous may be abused when it shields fraudulent conduct."); Udskey, *supra* note 5, at 884 (noting that an anonymous online speaker could "inflict serious harm on [a] corporation" by "polluting the information stream with defamatory falsehoods, which may in turn influence other investors to question the corporation's credibility or financial health").

[34] See Kang, *supra* note 23, at 1193 ("The potential for wide-ranging surveillance of all our cyber-activities presents a serious threat to information privacy."); cf. *McIntyre*, 514 U.S. at 355 (stating that the "identification of the author [of a political handbill] against her will is particularly intrusive ... [because] it reveals unmistakably the content of her thoughts on a controversial issue").

[35] Nicholas Carr, *The Great Privacy Debate: Tracking Is an Assault on Liberty, with Real Dangers*, Wall St. J., Aug. 7-8, 2010, at W1.

[36] See *Cahill v. Dorr*, 879 A.2d 943, 952 (Del. Super. Ct. 2005) ("If subpoenas can be obtained merely by filing suit, people will be reluctant to speak their mind knowing that their anonymity is tenuous and that retribution for whatever they might say is all the more likely."), *rev'd*, 884 A.2d 451 (Del. 2005); Udskey, *supra* note 5, at 861 ("Internet defamation actions threaten not only to deter the individual who is sued from speaking out, but also to encourage undue self-censorship among the other John Does who frequent Internet discussion fora.").

[37] This is not a novel concept, as some commentators have expressed support for recognizing an IP address as PII. See, e.g., Tene, *supra* note 18, at 1446 ("Even a dynamic address is personally identifiable in cyberspace, given the ability of a user's ISP to link such an address to the individual (or company) that used it."); see also Helms, *supra* note 9, at 296 ("One only needs the TCP/IP address and a cooperative ISP to link online activity to a user's biological identity.").

[38] See *infra* notes 49-75 and accompanying text.

[39] See *infra* notes 76-114 and accompanying text.

[40] See *infra* notes 118-30 and accompanying text.

[41] See *infra* notes 131-230 and accompanying text.

[42] See *infra* notes 231-63 and accompanying text.

[43] See *infra* notes 273-324 and accompanying text.

[44] See *infra* notes 325-50 and accompanying text.

[45] See *infra* notes 351-77 and accompanying text.

[46] See *infra* notes 49-75 and accompanying text.

[47] See *infra* notes 76-114 and accompanying text.

[48] See *infra* notes 82-97 and accompanying text.

[49] *United States v. Heckenkamp*, 482 F.3d 1142, 1144 n.1 (9th Cir. 2007). An example would be 74.125.95.99, which is the IP address assigned to one of the servers hosting <http://www.google.com> as of this writing.

[50] *Klimas v. Comcast Cable Commc's, Inc.*, 465 F.3d 771, 773 (6th Cir. 2006); *United States v. Steiner*, 318 F.3d 1039, 1042 (11th Cir. 2003).

[51] *Columbia Pictures Indus. v. Bunnell*, No. CV 06-1093 FMO/CX, 2007 WL 2080419, at 3 n.10 (C.D. Cal. May 29, 2007); see also Helms, *supra* note 9, at 296 n.44.

[52] See Alma Whitten, *Are IP Addresses Personal?*, Google Pub. Po'l'y Blog (Feb. 22, 2008, 12:31 PM), <http://googleregpublicpolicy.blogspot.com/2008/02/are-ip-addresses-personal.html> ("If you share your computer or even just your connection to your ISP with your family, then multiple people are sharing one IP address.").

[53] See *State v. Reid*, 945 A.2d 26, 33 (N.J. 2008).

[54] *Id.*

[55] See Gandy, *supra* note 14, at 1093.

[56] Kevin Werbach, *The Centripetal Network: How the Internet Holds Itself Together, and the Forces Tearing It Apart*, 42 U.C. Davis L. Rev. 343, 361 (2008).

[57] Due to the structure of IP addressing, certain addresses cannot be used on the Internet. This reduces the assignable address space from the theoretical maximum of more than four billion. See *id.*

[58] See *id.*; see also Lah, *supra* note 24, at 690.

[59] Warbach, *supra* note 56, at 361.

[60] See Lah, *supra* note 24, at 690.

[61] *Id.* at 690-91; Tene, *supra* note 18, at 1446. The protocol that enables dynamic addressing is known as DHCP, which stands for Dynamic Host Configuration Protocol. Lah, *supra* note 24, at 689.

[62] *State v. Reid*, 945 A.2d 26, 28 (N.J. 2008); *Cabill v. Doe*, 879 A.2d 943, 948 (Del. Super. Ct. 2005), *rev'd*, 884 A.2d 451 (Del. 2005).

[63] See Whitten, *supra* note 52.

[64] Helms, *supra* note 9, at 318. For the technical proposal, see Kjeld Borch Egevang & Paul Francis, The IP Network Address Translator (NAT) (Network Working Group, Request for Comments No. 1631) (May 1994), available at <http://www.ietf.org/rfc/rfc1631.txt>.

[65] Helms, *supra* note 9, at 318.

[66] See Jonathan Weinberg, Hardware-Based ID, Rights Management, and Trusted Systems, 52 *Stan. L. Rev.* 1251, 1260 n.22 (2000).

[67] Because the link is made with reference to a Media Access Control (MAC) address - a physical address that cannot normally be altered - the network administrator may track down an internal computer even if the internal address changes. See, e.g., *United States v. Mackenkarno*, 487 F.3d 1142, 1144 (9th Cir. 2007) (university's network investigator traced an internal IP address to a specific dorm room and then to a specific user even after the user had altered his internal address).

[68] See Paul Ham, Warrantless Search and Seizure of E-Mail and Methods of Panoptical Prophylaxis, B.C. L. Intell. Prop. & Tech. F. & J., Sept. 2008, at 1, 14.

[69] See *Id.*; Helms, *supra* note 9, at 318.

[70] Warbach, *supra* note 56, at 361.

[71] *Id.* at 361-62.

[72] Weinberg, *supra* note 66, at 1260-61; see also Helms, *supra* note 9, at 299 (indicating that the uniqueness of IPv6 addresses will "make it nearly impossible for people to remain anonymous on the Internet").

[73] How to Say the IPv6 Number, eLamb Security Blog (Dec. 12, 2006), <http://elamb.org/howto-say-the-ipv6-number>.

[74] See *supra* notes 49-55 and accompanying text.

[75] *United States v. Steiger*, 318 F.3d 1039, 1042 (11th Cir. 2003); *State v. Reid*, 945 A.2d 26, 29 (N.J. 2008).

[76] Lah, *supra* note 24, at 684.

[77] *Id.*; Berman & Mulligan, *supra* note 10, at 567; Norlan, *supra* note 28, at 811.

[78] 15 U.S.C. § 6501, 6502 (2006).

[79] 15 U.S.C. § 6502(a)(1); Corey A. Ciochetti, E-Commerce and Informational Privacy: Privacy Policies as Personal Information Protectors, 44 *Am. Bus. L.J.* 55, 75 (2007); Norlan, *supra* note 28, at 816-17.

[80] 18 U.S.C. § 2710 (2006).

[81] In 2008, the Southern District of New York refused to apply the Act when it compelled the production of logs linking YouTube visitors to their viewing records. *Viacom Int'l Inc. v. YouTube Inc.*, 253 F.R.D. 256, 262 & n.5 (S.D.N.Y. 2008); see also *infra* notes 361-68 and accompanying text.

[82] See S. Rep. No. 107-240, at 2-3 (2003) ("Taken together, these laws appear designed ... to ensure that certain types of information collection are fair, transparent, and subject to law.").

[83] Children's Online Privacy Protection Act of 1998, 15 U.S.C. § 6501(8)(A); False Identification Crime Control Act of 1982, 18 U.S.C. § 1028(d)(7)(A); Driver's Privacy Protection Act of 1994, 18 U.S.C. § 2725(3).

[84] 15 U.S.C. § 6501(8)(B); 18 U.S.C. § 2725(3).

[85] 15 U.S.C. § 6501(8)(C).

[86] 15 U.S.C. § 6501(8)(D); 18 U.S.C. § 2725(3).

[87] 15 U.S.C. § 6501(8)(E); 18 U.S.C. § 651026(d)(7)(A), 2725(3).

[88] 15 U.S.C. § 6501(8)(G).

89 15 U.S.C. § 6501(8)(F) (protecting as personal information "any other identifier that the Commission determines permits the physical or online contacting of a specific individual"). "Online contact information" is further defined as "an e-mail address or another substantially similar identifier that permits direct contact with a person online." § 6501(12).

90 18 U.S.C. § 1028(d)(7)(A).

91 18 U.S.C. § 2725(3).

92 Video Privacy Protection Act of 1988, 18 U.S.C. § 2710(a)(3).

93 16 U.S.C. § 1028(d)(7)(A), 2725(3).

94 § 1028(d)(7)(B).

95 § 1028(d)(7)(A).

96 Cable Communication Policy Act of 1984, 47 U.S.C. § 551(a)(2)(A) (2006).

97 See, e.g., *Id.*; see also 45 C.F.R. § 164.514(g) (2009) ("Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information.").

98 See Robert Sprague & Corey Ciochetti, Preserving Identities: Protecting Personal Identifying Information Through Enhanced Privacy Policies and Laws, 19 *Alb. L.J. Sci. & Tech.* 91, 118 (2009) (noting that the laws "miss a vast amount of data stored by merchants and various businesses"); Others have labeled the mass of statutes a "cobweb full of holes," Tene, *supra* note 18, at 1476, or a "patchwork" with "significant gaps," Norian, *supra* note 28, at 811.

99 See 18 U.S.C. § 2710(a)(3); 47 U.S.C. § 551(a)(2)(A).

100 15 U.S.C. § 6501(8); 18 U.S.C. § 2725(3).

101 18 U.S.C. § 1028(d)(7).

102 Thus, many scholars have used the statutes to craft their own definitions. See, e.g., Tene, *supra* note 18, at 1445 (defining PII as "information which can be used to uniquely identify, contact, or locate a specific individual person").

103 15 U.S.C. § 6501(8).

104 18 U.S.C. § 2725(3).

105 See Online Personal Privacy Act, S. 2201, 107th Cong. § 401 (2002); Consumer Privacy Protection Act of 2005, H.R. 4678, 107th Cong. § 401 (2002).

106 Ciochetti, *supra* note 79, at 98-99. For a comparison of the two bills, see Norian, *supra* note 28, at 822-27, 831-35.

107 Compare Online Personal Privacy Act, S. 2201 § 401 ("The term 'personally identifiable information' means individually identifiable information about an individual collected online ..."), with 15 U.S.C. § 6501(8) ("The term 'personal information' means individually identifiable information about an individual collected online ...").

108 S. 2201 § 401.

109 S. Rep. No. 107-240, at 40 (2002).

110 H.R. 4678 § 401(4A).

111 *Id.*

112 *In re The TJX Cos.*, No. 072 3055, at 2 (F.T.C. Mar. 27, 2008). In that case, an intruder breached TJX's insufficient electronic security measures and stole an estimated ninety-four million customer records, which contained credit card numbers, Social Security numbers, and driver's license numbers. Sprague & Ciochetti, *supra* note 98, at 97-100. See also Martin B. Robins, Intellectual Property and Information Technology Due Diligence in Mergers and Acquisitions: A More Substantive Approach Needed, 2008 *U. Ill. J.L. Tech. Pol'y* 321, 351 n.161 (indicating that the FTC's definition is "often used interchangeably" with statutory definitions of PII).

113 *In re The TJX Cos.*, No. 072 3055, at 2 (F.T.C. Mar. 27, 2008).

114 *Id.* A "cookie" is a file stored on the user's hard drive that contains a unique identifying number and other information, such as the user's preferred settings and the previous Web sites he visited. Michelle Z. Hall, Internet Privacy or Information Piracy: Spinning Lies on the World Wide Web, 18 *N.Y.L. Sch. J. Hum. Rts.* 609, 612-15 (2002). Cookies are a privacy concern because they can communicate a wealth of information to Web sites and may do so without the user's consent. *Id.*

115 See *infra* notes 167-230 and accompanying text.

116 See *infra* notes 131-66 and accompanying text.

117 See *infra* notes 118-30 and accompanying text.

118 See *supra* notes 76-111 and accompanying text.

119 See Article 29 Data Protection Working Party, Opinion 4/2007 on the Concept of Personal Data, 01248/07/EN/WP136, at 13-15 (June 20, 2007) [hereinafter WP136] (discussing how the ability of particular types of data to identify a person depends upon the circumstances).

120 Brief for Electronic Frontier Foundation as Amicus Curiae Supporting Defendant, *Kilmas v. Comcast Cable Commc'ns, Inc.*, (No. 02-CV-72054-DT), at 3-4, available at [http://w2.eff.org/Privacy/20040408 Kilmas v Comcast Amicus Brief.pdf](http://w2.eff.org/Privacy/20040408%20Kilmas%20v%20Comcast%20Amicus%20Brief.pdf) [hereinafter EFF Amicus Brief].

121 E-mail addresses may be shared, for example, by multiple people in one household (familyname@serviceprovider.com) or by multiple employees who sign in to a generic company account (info@company.com).

122 18 U.S.C. § 1028(d)(7)(A) (2006).

123 Sprague & Ciocchetti, *supra* note 98, at 93. A Social Security number is, of course, not intrinsically personally identifiable but is rather made so by accurately and consistently recording the link between the number and an individual. See Kang, *supra* note 23, at 1208. Thus, even this form of PII is not personally identifiable by itself.

124 18 U.S.C. § 1028(d)(7).

125 Compare 18 U.S.C. § 2725(3) (defining personal information as "information that identifies an individual" (emphasis added)), with H.R. 4678 § 401, 107th Cong. (2002) (defining PII as "information relating to a living individual who can be identified from that information" (emphasis added)). See also 45 C.F.R. § 164.514(a) (2009) (excluding from the definition of individually identifiable health information any data to which there is "no reasonable basis to believe that the information can be used to identify an individual" (emphasis added)).

126 See 1-2A Computer Law § 2A.02, at 16 (2009) ("A person can be identified ... by a combination of significant criteria that permits narrowing down the group to which he or she belongs ... Whether an individual is identified depends on the circumstances."); EFF Amicus Brief, *supra* note 120, at 5-8 (distinguishing "personally identifiable" from "personally identifying," the former being capable of identifying a person and the latter actually identifying a person).

127 What seems nonsensitive in isolation becomes sensitive in aggregation." Kang, *supra* note 23, at 1289 n.370. The danger aggregated data poses to individual privacy is demonstrated by a scandal involving the online video rental service, Netflix. In 2006, as part of a contest to improve its movie recommendation service, Netflix released 100 million records revealing the viewing and rating habits of 500,000 of its users. Arvind Narayanan & Vitaly Shmatikov, "Robust De-Anonymization of Large Sparse Datasets, 2008 IEEE Symp. on Security & Privacy 111, available at <http://www.cs.utexas.edu/shmat/shmat0808netflix.pdf>. The company had intended to remove all identifying information linking the habits to specific users, but a subsequent study showed that 84% of the users could be re-identified with the released data. *Id.* (concluding that, even if users are not overly concerned about the release of their movie ratings, the disclosure presented privacy concerns because "it is possible to learn sensitive non-public information about a person from his or her movie viewing history").

128 See WP136, *supra* note 119, at 15 ("If ... [the] possibility [to single out an individual] does not exist or is negligible, the person should not be considered as 'identifiable,' and the information would not be considered as 'personal data.'"); see also 45 C.F.R. § 164.514 (health privacy rule allowing release of medical information only after it is scrubbed of identifying data); H.R. 5777, 111th Cong. § 501(a)(2) (2010) (online privacy bill excluding from protection any information that has been obscured so as not to identify particular individuals).

129 See WP136, *supra* note 119, at 17 (reasoning that an ISP should protect IP addresses as personal data unless it knows "with absolute certainty" that a particular user cannot be identified).

130 See *supra* notes 82-97 and accompanying text.

131 See *supra* notes 49-55 and accompanying text.

132 See *Kilmas v. Comcast Cable Commc'ns, Inc.*, 465 F.3d 271, 276 n.2 (6th Cir. 2006).

133 *Id.* at 271.

134 *Id.* at 273.

135 *Id.* at 274.

136 *Kilmas v. Comcast Cable Commc'ns, Inc.*, No. 02-CV-72054-DT, 2003 U.S. Dist. LEXIS 27763, at 8 (E.D. Mich. July 1, 2003).

137 *Id.* at 10.

138 *Id.* at 10-11.

139 *Kilmas*, 465 F.3d at 273.

140 *Id.* at 276 n.2.

141 *Id.* at 276-280.

142 *Id.* at 280 (quoting 47 U.S.C. § 551(a)(2)(A) (2006)).

143 ⁷Id.

144 ⁷See 1-2A Computer Law § 2A:02 n.4 ("An IP address standing alone would merit only the lowest degree of security."); see also Whitten, *supra* note 52 ("The IP addresses recorded by every Web site on the planet without additional information should not be considered personal data, because these Web sites usually cannot identify the human beings behind these number strings.").

145 ⁷See *supra* notes 61-63 and accompanying text.

146 ⁷See Lah, *supra* note 24, at 639; Weinberg, *supra* note 66, at 1260 & n.24; see also *United States v. Vosturnh*, 602 F.3d 512, 523 (1st Cir. 2010) ("Comcast's ... 'lease period' for each IP address is approximately 6-8 days. At the expiration of that lease period, the assignment of an address to a particular computer may or may not be renewed.").

147 ⁷*Kilmas*, 465 F.3d at 276 n.2.

148 ⁷See Tene, *supra* note 18, at 1446 (comparing IP addresses to mailing addresses and telephone numbers, which are PII only when they "might be linked to a specific individual through reasonable means").

149 ⁷See EFF Amicus Brief, *supra* note 120, at 3 ("Without the equivalent of a reverse telephone directory, a person's telephone number is just a telephone number.").

150 ⁷Id.

151 ⁷See *id.*

152 ⁷*Columbia Pictures Indus. v. Bunnell*, No. CV-06-1093 FMCJX, 2007 WL 2080419, at 3 n.10 (C.D. Cal. May 29, 2007). The court examined the question under the defendant's privacy policy rather than a federal statute. *Id.* Problematically, the defendant did not provide the court with a definition of the term "personal information" as used in its policy. *Id.*

153 ⁷*Johnson v. Microsoft Corp.*, No. C06-0900RAJ, 2009 U.S. Dist. LEXIS 58174, at 13 (W.D. Wash. June 23, 2009).

154 ⁷Id. at 12-13.

155 ⁷See *supra* notes 82-97 and accompanying text.

156 ⁷See *Bunnell*, 2007 WL 2080419, at 3 n.10; Helms, *supra* note 9, at 296 n.46.

157 ⁷Therefore, an address may not be personally identifiable in some circumstances, such as when it identifies an apartment building but not the particular apartment. See Tene, *supra* note 18, at 1446.

158 ⁷When a telephone is available for use by more than one person, the calls made from the telephone are less likely to be fairly attributable to an individual. See Nancy J. King, When Mobile Phones Are RFID - Equipped: Finding E.U.-U.S. Solutions to Protect Consumer Privacy and Facilitate Mobile Commerce, 15 *Mich. Technol. & Tech. L. Rev.* 107, 181 n.287 (2008).

159 ⁷See WP136, *supra* note 119, at 13 ("The question of whether the individual to whom the information relates is identified or not depends on the circumstances of the case.").

160 ⁷See King, *supra* note 158, at 181 n.287.

161 ⁷See Sprague & Clocchetti, *supra* note 98, at 93.

162 ⁷Latanya Sweeney, Computational Disclosure Control: A Primer on Data Privacy Protection 20 (Jan. 8, 2001), available at <http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/sweeney-thesis-draft.pdf>; see also Seth Schoen, What Information Is "Personally Identifiable"? Electronic Frontier Foundation (Sept. 11, 2009), <http://www EFF.org/Deadlines/2009/09/what-information-personally-identifiable>; Kang, *supra* note 23, at 1289 n.370 ("The true privacy threat arises from the systematic, detailed aggregation of otherwise trivial data that allows the construction of a telling personal profile.").

163 ⁷See Clocchetti, *supra* note 79, at 56.

164 ⁷Compare Gandy, *supra* note 14, at 1093 ("It is in the nature of the Internet Protocol (IP) that personally identifiable information is made available for capture in every interaction between computers."), with King, *supra* note 158, at 181 ("Certain types of IP addresses that do not allow identification of the user may not be personal data.").

165 ⁷See EFF Amicus Brief, *supra* note 120, at 9.

166 ⁷See Berman & Mulligan, *supra* note 10, at 554 (noting online transactional data, such as IP address and Web site history, can "reveal the blueprint of an individual's life").

167 ⁷See *supra* notes 60-63 and accompanying text.

168 ⁷See, e.g., *Kilmas v. Comcast Cable Commc'ns, Inc.*, No. 02- CV-72054-GT, 2003 U.S. Dist. LEXIS 27765, at 10 (E.D. Mich. July 1, 2003).

169 ⁷See *supra* notes 64-66 and accompanying text.

[170] An IP address is tied to a specific computer when the computer uses a static, public IP address. Lali, *supra* note 24, at 690.

[171] See *infra* notes 205-24 and accompanying text.

[172] *United States v. Steiner*, 318 F.3d 1039, 1042 (11th Cir. 2003).

[173] See *Klimas v. Comcast Cable Comm'ns. Inc.*, 465 F.3d 271, 273 (6th Cir. 2006); *United States v. Kennedy*, 81 F. Supp. 2d 1103, 1108 (D. Kan. 2000).

[174] See, e.g., *United States v. Vosburgh*, 602 F.3d 512, 522 (3d Cir. 2010) (noting that the defendant's ISP maintained IP assignment logs for 180 days). Note, however, that the FBI is currently pressuring ISPs to retain assignment logs for as long as two years. Declan McCullagh, FBI Wants Records Kept of Web Sites Visited, CNET News (Feb. 5, 2010, 9:16 AM), <http://news.cnet.com/8301-13578-3-10448060-38.html>.

[175] Weinberg, *supra* note 66, at 1260 n.24.

[176] *Id.*

[177] Tene, *supra* note 18, at 1446.

[178] *United States v. Vosburgh*, 602 F.3d 512, 522 (3d Cir. 2010).

[179] *Id.* at 517.

[180] *Id.*

[181] *Id.* at 523.

[182] *Id.*

[183] *United States v. Steiner*, 318 F.3d 1039, 1042 (11th Cir. 2003).

[184] *Id.*

[185] *Id.*

[186] *Id.* at 1043, 1045.

[187] See *In re Charter Comm'ns. Inc.*, 393 F.3d 771 (8th Cir. 2005).

[188] *Id.* at 774.

[189] *Id.*

[190] *Id.*

[191] *Id.* The opinion does not explain the discrepancy between the number of subscribers originally identified by Charter and the number subpoenaed. See *id.*

[192] *Id.* at 777.

[193] *Id.* at 778.

[194] See Weinberg, *supra* note 66, at 1260 n.22 ("The extent to which ... traffic can be traced to [a user behind NAT] ... depends on the information retained by that server.").

[195] See Egevang & Francis, *supra* note 64, at 1.

[196] See *United States v. Heckenkamp*, 482 F.3d 1142, 1148 (9th Cir. 2007).

[197] See Weinberg, *supra* note 66, at 1260 n.22.

[198] See generally Heckenkamp, 482 F.3d at 1142.

[199] *Id.* at 1143.

[200] *Id.*

[201] *Id.* at 1144.

[202] *Id.*

203 Id. at 1145.

204 Id.

205 See WP136, *supra* note 119, at 17 (presenting the scenario of an anonymous user of a computer in an Internet cafe).

206 See King, *supra* note 158, at 181; see also WP136, *supra* note 119, at 17.

207 This scenario would be identical to that of the office telephone to which multiple people have easy access. See King, *supra* note 158, at 181 n.287.

208 Kang, *supra* note 23, at 1226; see also Christopher Kuner, European Data Privacy Law & Online Business 50 (2003).

209 Kuner, *supra* note 208, at 50.

210 Id.

211 See *United States v. Kennedy*, 81 F. Supp. 2d 1103, 1107, 1114 (D. Kan. 2000) (finding the defendant's admission that he was the primary user of an Internet account provided probable cause for a search of his computer).

212 *United States v. Voshburgh*, 602 F.3d 512, 576 (3d Cir. 2010) (noting that "several Courts of Appeals have held that evidence that the user of a computer employing a particular IP address possessed or transmitted child pornography can support a search warrant for the physical premises linked to that IP address"); *United States v. Skults*, 575 F.3d 834, 844 (8th Cir. 2009); *United States v. Perrine*, 518 F.3d 1196, 1199-1200, 1206 (10th Cir. 2008); *United States v. Perez*, 484 F.3d 735, 740 (5th Cir. 2007); *United States v. Winters*, 452 F.3d 534, 539 (6th Cir. 2006); *United States v. Hay*, 231 F.3d 630, 635-36 (9th Cir. 2000).

213 *Perez*, 484 F.3d at 735.

214 Id. at 738.

215 Id. at 738, 741.

216 Id. at 742.

217 Id. at 744.

218 Id. at 740 (emphases added).

219 *United States v. Kennedy*, 81 F. Supp. 2d 1103 (D. Kan. 2000).

220 Id. at 1106-07.

221 Id.

222 Id. at 1107-08.

223 The FBI also determined that the defendant liked to download pictures from the Internet and was suspicious that others were reading his computer files. Id. at 1107. This information was obtained in a pretextual phone call in which the FBI agent pretended to be a representative of the defendant's ISP. Id. at 1114.

224 Id.

225 For a useful visual representation of the technical process used to trace IP address assignments, see Helms, *supra* note 9, at 296.

226 See Aolfe White, IP Addresses Are Personal Data, E.U. Regulator Says, Wash. Post, Jan. 22, 2008, at D1 (paraphrasing Germany's data-protection commissioner as saying "when someone is identified by an IP ... address, 'then it has to be regarded as personal data'").

227 See *In re Charter Commc'ns. Inc.*, 393 F.3d 771, 774 (8th Cir. 2005).

228 See *supra* notes 140-50 and accompanying text.

229 See *Klimas v. Comcast Cable Commc'ns. Inc.*, No. 02- CV-72054-DT, 2003 U.S. Dist. LEXIS 27765, at 10 (E.D. Mich. July 1, 2003) ("Unless an IP address is correlated to some other information ... it does not identify any single subscriber by itself.").

230 See *supra* notes 77-81 and accompanying text (discussing the limited scope of federal privacy law).

231 See Conn. Gen. Stat. § 54-260b (2009); Ind. Code § 35-37-6-2.5 (1998); Minn. Stat. § 325M.01-09 (2004); Mont. Code Ann. § 2-17-551 (2009); Wis. Stat. § 19.68 (2003).

232 Ind. Code § 35-37-6-2.5.

233 Ind. Code § 35-37-6-2.5(a).

[234] Conn. Gen. Stat. § 54-260b (2009).

[235] Minn. Stat. § 325M.02-04; see also Jordan M. Blanke, Minnesota Passes the Nation's First Internet Privacy Law, 29 Rutgers Computer & Tech. L.J. 405, 405-413 (2003). The statute also protects "clickstream data," data that indicates where a user has been and how he found the current Web site. Blanke, *supra*, at 409-09 & n.18.

[236] Minn. Stat. § 325M.01 (emphasis added).

[237] See Minn. Stat. § 325M.02.

[238] Minn. Stat. § 325M.03(6), (7).

[239] 45 C.F.R. § 164.514(b)(2)(i)(O) (2009).

[240] 45 C.F.R. § 164.514(b).

[241] *Id.*

[242] *Id.* § 164.514(b)(2)(i)(O).

[243] H.R. 5777, 111th Cong. (2010). Behavioral advertising, also known as behavioral targeting, "is a method of tracking the online behavior of Internet users in order to serve those consumers with advertising targeted to the specific interests 'expressed' through Web-browsing activity." Andrew Hotaling, Protecting Personally Identifiable Information on the Internet: Notice and Consent in the Age of Behavioral Targeting, 16 Comm. Law Conspectus 529, 530 (2008). Behavioral advertising is a controversial practice because of the challenge to expectations of privacy online. *Id.*

[244] H.R. 5777 § 2(4)(vii).

[245] US Lawmakers Publish Internet Privacy Bill, The Register (May 6, 2010, 8:13 AM), <http://www.theroaster.co.uk/2010/05/06/internet-privacy-bill/>.

[246] "Covered entity" is defined as "a person engaged in interstate commerce that collects or stores data containing covered information or sensitive information," except for government entities and any person who (i) stores information from fewer than 15,000 individuals, (ii) collects information from fewer than 10,000 persons in a twelve-month period, (iii) does not collect sensitive information, and (iv) does not use the information to study individuals as its primary business. H.R. 5777 § 2(3).

[247] *Id.* §§ 101-103.

[248] *Id.* § 104(a)(1).

[249] *Id.* § 106.

[250] *Id.* § 103(e).

[251] See *id.* § 2(5)(A) (defining "operational purpose" in part as "a purpose reasonably necessary to facilitate ... the logistical or technical ability of a covered entity to provide goods or services").

[252] See *id.* § 2(5)(B) (defining "operational purpose" to exclude information used for a marketing or advertising purpose or any purpose that "would likely affect the individual's conduct or decisions with respect to the covered entity's products or services").

[253] Article 29 Data Protection Working Party, Opinion 1/2008 on Data Protection Issues Related to Search Engines, 00737/EN/WP148, at 3, 8 (Apr. 4, 2008) [hereinafter WP148]. For a more detailed analysis of the EU's approach, see Lah, *supra* note 24, at 695-99.

[254] WP148, *supra* note 253, at 8.

[255] *Id.* at 19-21. See Lah, *supra* note 24, at 696.

[256] EMI Records Ltd. v. Eircom Ltd., [2010] I.E.H.C. 108 (Ire.).

[257] *Id.* P 1.

[258] *Id.* PP 2, 9.

[259] *Id.* P 16.

[260] *Id.* P 19: Note that this definition protects both data that actually identify an individual and data that could identify an individual if correlated to other data in the party's possession.

[261] *Id.* P 25.

[262] *Id.*

263 Id. P-12.

264 See infra notes 351-68 and accompanying text.

265 See infra notes 369-75 and accompanying text.

266 See infra notes 331-74 and accompanying text.

267 See infra notes 276-87 and accompanying text.

268 See, e.g., 15 U.S.C. § 6501(B)(F) (2006) (protecting "any other identifier that the Commission determines permits the physical or online contacting of a specific individual").

269 See infra notes 325-50 and accompanying text.

270 See, e.g., United States v. Bynum, 604 F.3d 151, 164 (4th Cir. 2010) (holding that an Internet user did not have an objectively reasonable expectation of privacy in the information on file with his ISP, including his name, e-mail address, telephone number, and physical address).

271 See State v. Reid, 195 A.2d 26, 33 (N.J. 2008).

272 See infra notes 273-322 and accompanying text.

273 See Columbia Ins. Co. v. Seascandy.com, 185 F.R.D. 573, 577-78 (N.D. Cal. 1999).

274 Spencer, supra note 29, at 495. See, e.g., Doe v. Cahill, 804 A.2d 451, 455 (Del. 2005); Solars, Inc. v. Doe, 977 A.2d 951, 944 (D.C. Cir. 2009).

275 See, e.g., 18 U.S.C. § 2710(b)(2)(F) (2006) (requiring a showing of "compelling need" before a subpoena may issue).

276 See Spencer, supra note 29, at 493.

277 17 U.S.C. § 512(h)(1) (2006).

278 § 512(h)(4).

279 § 512(h)(5).

280 See Charter Communications, 393 F.3d at 777 (holding that the DMCA does not authorize the issuing of a subpoena when the ISP merely acts as a "conduit" to infringing conduct).

281 18 U.S.C. § 2710(b)(2)(F) (2006).

282 § 2710(b)(2)(D).

283 47 U.S.C. § 551(c)(2)(B) (2006).

284 § 551(h).

285 18 U.S.C. § 2703(c).

286 § 2703(d).

287 18 U.S.C. § 2702(c)(6); United States v. Hambrick, 55 F. Supp. 2d 504, 507 (W.D. Va. 1999) ("The ECPA's concern for privacy extends only to government invasions of privacy. ISPs are free to turn stored data and transactional records over to nongovernmental entities.").

288 See Doe v. Individuals Whose True Names Are Unknown, 561 F. Supp. 2d 249, 254 (D. Conn. 2008); Columbia Ins. Co. v. Seascandy.com, 185 F.R.D. 573, 578 (N.D. Cal. 1999).

289 See Michael S. Vogel, Unmasking "John Doe" Defendants: The Case Against Excessive Hand-Wringing over Legal Standards, 83 Or. L. Rev. 795, 807-08 (2004).

290 Seascandy.com, 185 F.R.D. at 578; Spencer, supra note 29, at 499.

291 See Seascandy.com, 185 F.R.D. at 578 ("People who have committed no wrong should be able to participate online without fear that someone who wishes to harass or embarrass them can file a frivolous lawsuit and thereby gain the power of the court's order to discover their identity."); Spencer, supra note 29, at 498 (discussing a case in which an employer discovered the identities of twenty-one online speakers, dropped its trade secret suit, and fired the four who were its employees).

292 See Doe v. Individuals, 561 F. Supp. 2d at 255 (reviewing subpoena standards for unmasking an anonymous defendant). For further analysis of this line of cases, see generally Mazzotta, supra note 32, at 833, and Ryan M. Martin, Freeing the Net: Rejecting a One-Size-Fits-All Standard for Unmasking Anonymous Internet Speakers in Defamation Lawsuits, 75 U. Chi. L. Rev. 1217 (2007).

[293] See v. Cahill, 884 A.2d 451, 458 (Del. 2005). When a plaintiff shows sufficient evidence of a defamation claim, however, further balancing against a defendant's free speech interest is unnecessary because truly defamatory speech is not protected by the First Amendment. Beauharnais v. Illinois, 343 U.S. 250, 256 (1952); Sellers, Inc. v. Doe, 977 A.2d 941, 956 (D.C. Cir. 2009).

[294] See In re Subpoena Duces Tecum to Am. Online, Inc., No. 40570, 2000 WL 1210372, at 6 (Va. Cir. Ct. Jan. 31, 2000), rev'd on other grounds, 542 S.E.2d 377 (Va. Ct. App. 2001).

[295] Id. at 7.

[296] Martin, supra note 292, at 1220.

[297] For further examination of subpoena standards in defamation cases, see Id. at 1228-37.

[298] Am. Online, 2000 WL 1210372, at 8.

[299] Id. at 1.

[300] Id. at 6.

[301] Id. at 7.

[302] Id.

[303] See Doe v. Individuals Whose True Names Are Unknown, 561 F. Supp. 2d 249, 255 (D. Conn. 2009); Doe v. Cahill, 884 A.2d 451, 458 (Del. 2005).

[304] Cahill, 884 A.2d at 461.

[305] Id. at 454.

[306] Id. at 455.

[307] Id. at 457.

[308] Id.

[309] Id. at 458, 461. The court relied heavily upon a similar standard imposed by the Superior Court of New Jersey in the case Dendrite International, Inc. v. Doe, 775 A.2d 756 (N.J. Super. Ct. App. Div. 2001).

[310] Cahill, 884 A.2d at 461.

[311] Id. at 464. The court noted that it could be difficult or impossible to prove a defendant's actual malice without discovering the defendant's identity. Id. Therefore, proof of that element of a public figure's defamation claim could be postponed, and the plaintiff would only be required to show proof of elements within its control. See Id.

[312] See Sellers, Inc. v. Doe, 977 A.2d 941 (D.C. Cir. 2009).

[313] Id. at 944-45.

[314] Id. at 957.

[315] Id. at 952.

[316] Id. at 954.

[317] This factor is easily satisfied when the anonymous speaker the plaintiff seeks to identify is the defendant, for the plaintiff cannot proceed with his action until he knows who the defendant is. Id. at 955.

[318] See Id. at 954.

[319] Columbia Ins. Co. v. Seegranly.com, 185 F.R.D. 573 (N.D. Cal. 1999).

[320] Id. at 575-76.

[321] See Id. at 579. The court's full test contained four prongs, requiring the plaintiff to (1) "identify the missing party with sufficient specificity such that the Court can determine that defendant is a real person," (2) "identify all previous steps taken to locate the elusive defendant," (3) establish that the case could withstand a motion to dismiss, and (4) file a discovery request with the court identifying the persons on whom discovery could be served. Id. at 576-80.

[322] See Id. at 579-80. The motion to dismiss standard has been criticized as potentially confusing because of variations in standards across jurisdictions. Doe v. Individuals Whose True Names Are Unknown, 561 F. Supp. 2d 249, 255 (D. Conn. 2009).

[323] See Mazzotta, *supra* note 32, at 846.

[324] *Id.* at 847-56.

[325] For more on Fourth Amendment protections online, see generally Solove, *supra* note 9, at 1083, and Orin S. Kerr, Applying the Fourth Amendment to the Internet: A General Approach, 62 *Stan. L. Rev.* 1005 (2010).

[326] See, e.g., *United States v. Byrum*, 604 F.3d 161, 164 (4th Cir. 2010).

[327] See *id.*

[328] *Id.* (quoting *United States v. Perrine*, 518 F.3d 1196, 1204 (10th Cir. 2008)); see also Kerr, *supra* note 325, at 1026 ("Courts ... have uniformly concluded that the Fourth Amendment does not protect [basic subscriber information]").

[329] See David A. Coullard, Note, Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing, 93 *Minn. L. Rev.* 2205, 2227 (2009).

[330] *Byrum*, 604 F.3d at 164 (alterations omitted) (internal quotations omitted) (quoting *Smith v. Maryland*, 442 U.S. 735, 744 (1979)); see, e.g., *Guest v. Leis*, 255 F.3d 325, 336 (6th Cir. 2001) (concluding that "computer users do not have a legitimate expectation of privacy in their subscriber information because they have conveyed it to another person - the system operator").

[331] See Coullard, *supra* note 329, at 2214-15, 2227; Robert A. Piskowsky, An Overview of the Law of Electronic Surveillance Post-September 11, 2001, 94 *U. Ill. L. Rev.* 601, 608 (2002).

[332] The lethargic way in which courts have approached Fourth Amendment concerns online is certainly not unprecedented: "It took the Supreme Court until 1967 - nearly a full century after the invention of the telephone - to recognize telephone conversations as constitutionally protected against unreasonable searches." Coullard, *supra* note 329, at 2206.

[333] *City of Ontario v. Quon*, 130 S. Ct. 2619, 2629 (2010).

[334] See Kerr, *supra* note 325, at 1006-07.

[335] *Olmstead v. United States*, 277 U.S. 478 (1928).

[336] *Id.* at 474 (Brandeis, J., dissenting).

[337] Daniel J. Solove, Reconstructing Electronic Surveillance Law, 72 *Geo. Wash. L. Rev.* 1764, 1787 (2004).

[338] To sign up for [Internet] service, a customer must disclose personal information including one's name, billing information, phone number, and home address." *State v. Reid*, 945 A.2d 26, 28 (N.J. 2008) (emphasis added).

[339] *Id.* at 26.

[340] *Id.* at 28.

[341] *Id.* at 27.

[342] *Id.*

[343] *Id.* at 27, 29-30.

[344] *Id.* at 30.

[345] *Id.* at 32.

[346] *State v. Hunt*, 450 A.2d 952 (N.J. 1982).

[347] *Reid*, 945 A.2d at 32.

[348] *Id.* at 33.

[349] *Id.*

[350] Kerr, *supra* note 325, at 1006-07.

[351] 15 U.S.C. § 6501(b)(F) (2006).

[352] 18 U.S.C. § 1028(d)(7)(C) (2006).

[353] Orin S. Kerr, A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It, 72 Geo. Wash. J. Rev. 1208, 1219-20 (2004).

[354] 18 U.S.C. § 2703(c)(2).

[355] See Kerr, *supra* note 353, at 1234.

[356] See EFF Amicus Brief, *supra* note 120, at 4 (noting that the IP information at issue in the Kilmas case "included information about what subscribers communicated, viewed or read on-line").

[357] See *supra* notes 273-87 and accompanying text.

[358] Leh, *supra* note 24, at 684; Berman & Mulligan, *supra* note 10, at 576.

[359] 17 U.S.C. § 512(h)(4) (2006).

[360] See 18 U.S.C. § 2710(b)(2)(F) (2006).

[361] *Viacom Int'l Inc. v. YouTube Inc.*, 253 F.R.D. 256 (S.D.N.Y. 2008).

[362] *Id.* at 258-59.

[363] *Id.* at 261.

[364] *Id.* at 262.

[365] *Id.*

[366] *Id.*

[367] See *supra* notes 187-93 and accompanying text (discussing a case in which the RIAA sought to use IP addresses to expose the identities of alleged downloaders of copyrighted music).

[368] See Patricia Sanchez Abri & Anita Cava, Health Privacy in a Techno-Social World: A Cyber-Patient's Bill of Rights, 6 Nw. J. Tech. & Intell. Prop. 244, 251 (2008) (expressing concern that the decision could set precedent requiring social networking Web sites to disclose their users' computer locations and online activities).

[369] See Couillard, *supra* note 329, at 2229 (discussing how the transactional nature of IP addresses may be conflated with the content of Internet communications).

[370] See *supra* notes 304-18 and accompanying text.

[371] *Sales, Inc. v. Dor.* 977 A.2d 941, 955 (D.C. Cir. 2009).

[372] See *Doe v. Cahill*, 884 A.2d 451, 462 (Del. 2005) (adopting a summary judgment standard as the proper balance between the parties' interests).

[373] *Accord id.*

[374] See Couillard, *supra* note 329, at 2215; cf. *Smith v. Maryland*, 442 U.S. 747 (1979) ("We doubt that people in general entertain any actual expectation of privacy in the [telephone] numbers they dial.").

[375] See *Smith*, 442 U.S. at 743 (distinguishing between the telephone number dialed, to which the user had no reasonable expectation of privacy, and the contents of the communication); Couillard, *supra* note 329, at 2229.

[376] See Weinberg, *supra* note 66, at 1260-61.

[377] See *id.*

[378] Vogel, *supra* note 289, at 814.

[379] Tene, *supra* note 19, at 1455.

[380] See Vogel, *supra* note 289, at 803; Ham, *supra* note 68, at 20.

[381] See Mazzotta, *supra* note 32, at 855.

[382] See *supra* notes 286-322 and accompanying text.

[383] See EFF Amicus Brief, *supra* note 120, at 9.

Jump To ▾



► LexisNexis

ARTICLE: Accessing the Internet Through the Neighbor's Wireless Internet Connection: Physical Trespass in Virtual Reality, 84 Neb. L. Rev. 1226

Copy Citation

2006

Reporter

84 Neb. L. Rev. 1226

Length: 20924 words

Author: Ned Snow*

© Copyright held by the NEBRASKA LAW REVIEW

*B.A. 2000, summa cum laude, Brigham Young University; J.D. 2003, Harvard Law School. The following persons provided helpful assistance in researching and drafting this Article: Gove Allen, Amy Benson, Jeremy Fielding, Michael Hilgers, Eirik Leerskov, John Nickelson, and Doug Stallings. The Author also thanks his wife, Elissa, for her tremendous support of his scholarship.

Document: ARTICLE: Accessing the Internet Through the Neighbor's Wir... Actions ▾

LexisNexis Summary

... Wireless fidelity ("Wi-Fi") technology brings the Internet anywhere that a radio signal can reach. ... Applying this new doctrine to the Wi-Fi context reveals that a joyriding neighbor likely trespasses when the neighbor sends electronic signals to the Wi-Fi operator's device that transmits data through the Internet - a Wi-Fi router. ... Part IV examines the defenses to trespass to chattel, addressing whether joyriding is permissible when a Wi-Fi operator has not password protected the network or when the Wi-Fi operator's network interferes with the neighbor's ability to set up his or her own wireless network. ... If a joyriding neighbor only surfs the web or checks e-mail, the Wi-Fi operator's rate of data transmission to and from the Internet is not noticeably slower than if the neighbor were not using the wireless network. ... If the joyriding neighbor commits a trespass to chattel against the Wi-Fi operator, the Wi-Fi operator must own a "thing" on which a trespass can be committed. ... According to this recent Internet jurisprudence, the radio signals that a joyriding neighbor sends to a Wi-Fi operator's router appear to constitute trespassory harm. ... A joyriding neighbor appears to trespass on the Wi-Fi operator's router. ...

Text

[1227]

I. INTRODUCTION

Wireless fidelity ("Wi-Fi") technology brings the Internet anywhere that a radio signal can reach. [1±] Transmitting radio signals beyond the confines of walls, fences, and property lines, Wi-Fi technology delivers newfound convenience to a person who operates a wireless computer network ("Wi-Fi operator"). [2±] This convenience, however, has given rise to an unintended externality. Persons whom the Wi-Fi operator never intended to receive the transmission may realize full Internet access at the operator's expense. [3±] A Wi-Fi operator pays \$ 29.95 each month for Internet service; [4±] the operator's next-door neighbor reaps that same service for free. [5±] In the lexicon of cyber speech, this phenomenon is appropriately referred to as "joyriding." [6±] Joyriding can cause substantial delays in data transmission, [7±] and it can facilitate the diffusion of harmful viruses to all computers within the wireless network. [8±] Yet despite these possible harms, Wi-Fi operators often do [1228] not password protect their networks. [9±] Joyriding has thus become common practice. [10±] The law should intervene. [11±]

The question of whether the common law permits a neighbor to joyride on a wireless network presents novel and complex issues of tort and property law. [12±] At first glance, it seems that the joyriding neighbor does not invade any legally protected interest of the Wi-Fi operator, even though the Wi-Fi operator may suffer negative externalities. [13±] Tort law does not appear to protect a Wi-Fi operator's interest in the wireless network because a wireless network comprises radio signals. [14±] Radio signals are uncontrollable by nature, and thereby cannot be property. [15±] Absent property, trespass cannot lie. [16±]

[1229] Even if wireless networks were recognized as property, the neighbor's conduct is arguably permissible. Where the Wi-Fi operator has failed to set up a password, the operator seems to implicitly consent to sharing Internet access. [17±] The Wi-Fi operator seems to consent to joyriding. [18±] Furthermore, the common law permits a neighbor to use property that crosses onto and interferes with the neighbor's airspace. [19±] The Wi-Fi radio signals cross over to the neighbor's land, potentially interfering with the neighbor's airspace, so the common law may protect the neighbor's conduct. [20±] Finally, social policy seems to support the position of the joyriding neighbor. The Internet is a public good, and the law should support any means of allowing as many persons to access it. [21±] To that end, it is arguable that Wi-Fi radio signals, which travel over government-regulated frequencies, [22±] should not be subject to private ownership. Wi-Fi signals should arguably be treated as part of a public commons available for anyone's use. [23±]

Despite these arguments against finding a trespass, recent caselaw dealing with the Internet suggests otherwise. Courts are quickly remolding the age-old trespass-to-chattel doctrine so that it fits the new medium of cyberspace. [24±] Albeit relatively young, Internet jurisprudence [1230] has espoused the view that electronic signals sent through cyberspace to a physical object may give rise to contact that is [25±] sory in nature. [25±] Applying this new doctrine to the Wi-Fi context reveals that a joyriding neighbor likely trespasses when the neighbor sends electronic signals [26±] to the Wi-Fi operator's device that transmits data through the Internet - a Wi-Fi router. [26±] Whereas Wi-Fi radio signals are not property, the Wi-Fi router indisputably is. It is a physical object that remains in the possession and control of the Wi-Fi operator.

R.A. / 86

[27] Under the reasoning of Internet caselaw, the joyriding neighbor appears to "intermeddle" with the router when the neighbor sends electronic signals through it. [28] Because the router is the property under consideration - rather than Wi-Fi radio signals - the fact that a joyriding neighbor uses Wi-Fi radio signals which cross over to the neighbor's land is of no consequence. [29] Trespassory contact appears to occur at the router.

Policy also implies a trespass. The transaction costs of joyriding - the possibility of computer viruses and transmission delays - outweigh the benefit of permitting joyriding neighbors free access to the Internet. [30] In short, joyriding can impose costly consequences on the unsuspecting Wi-Fi operator. [31] Moreover, even if these transaction costs did not exist, the joyriding neighbor strips Internet service providers ("ISPs") of economic returns. [32] It is likely that some joyriding neighbors value Internet access at a level sufficiently high such that they would subscribe to ISP services were joyriding unavailable. [33] To realize a full return on their investment in Internet technology, ISPs must receive payment for their services by anyone who uses it. Protection [1231] of Internet investments favors viewing the neighbor's conduct as a trespass. [34]

This Article addresses the question of whether the joyriding neighbor commits an actionable trespass against the Wi-Fi operator. Part II explains how a wireless network functions, and how a neighbor is able to access that network. Part III examines whether the neighbor's conduct satisfies the elements of trespass to chattel, identifying the chattel at issue as the Wi-Fi router. Part III concludes that the neighbor's conduct satisfies the elements of trespass to chattel. Part IV examines the defenses to trespass to chattel, addressing whether joyriding is permissible when a Wi-Fi operator has not password protected the network or when the Wi-Fi operator's network interferes with the neighbor's ability to set up his or her own wireless network. Part IV concludes that neither the absence of password protection nor the presence of Wi-Fi interference should be a defense to the tortious conduct.

II. FACTUAL BACKGROUND

A wireless network allows computers within a local geographic area to share information without being connected by wires. [35] Radio signals make Wi-Fi technology possible. [36] Wi-Fi radio signals originate from a device called a Wi-Fi router. [37] The Wi-Fi router transmits data between computers within the network, and between a modem that is connected to the Internet and a computer within the network. [38] In effect, the Wi-Fi router serves as a hub for information exchange between computers within the network and between any network computer and the Internet. [39]

Wi-Fi routers operate on frequencies that the government has permitted consumers to use without licenses. Baby monitors, cordless phones, microwave ovens, Bluetooth devices, [40] and other wireless devices [1232] all operate on the same unlicensed frequencies as Wi-Fi routers. [41] To prevent wireless devices from interfering with one another, the frequencies have multiple channels on which a single wireless device can operate. [42] Most wireless devices will "listen" for a clear channel before becoming active. [43] Thus, a wireless network can experience interference, but technological advances are decreasing instances of such interference.

The range of a Wi-Fi router's signal varies according to its strength in relation to physical obstructions. [44] On average, routers can reliably transmit signals over a range of about 300 feet, approximately the size of a football field. [45] Physical objects cannot usually impede Wi-Fi radio signals anywhere within this range. [46] Hence, data transmission is possible between computers in separate rooms, or even in different buildings. [47]

The strength of Wi-Fi radio signals allows a neighbor of a Wi-Fi operator to access the wireless network. [48] The neighbor need merely install a wireless network adapter on a computer and place the computer within the range of the Wi-Fi operator's router. [49] After the wireless network adapter is installed on the neighbor's computer, the computer can receive Wi-Fi radio signals. [50] When the computer locates a Wi-Fi signal, it displays a prompt on its screen, querying the neighbor whether the computer should interface with the wireless network. [51] [1233] Selecting "OK" connects the neighbor's computer to the Internet through the wireless network. [52] A neighbor might view websites, check e-mail, download files, file share, or media stream. [53] Any of these practices constitutes "joyriding." [54] It is noteworthy that while joyriding, a neighbor may unintentionally transmit an electronic virus to computers within the wireless network. [55] That is, a virus can pass from the neighbor's computer, through the router, to the operator's computer - even where the neighbor does not access the operator's computer, but merely accesses the Internet through the Wi-Fi connection. [56] In the absence of specialized software that many Wi-Fi operators are not likely aware of, viruses within a network can spread uninhibited from computer to computer. [57]

A Wi-Fi operator often does not know when someone is joyriding on the wireless network. [58] If a joyriding neighbor only surfs the web or checks e-mail, the Wi-Fi operator's rate of data transmission to and from the Internet is not noticeably slower than if the neighbor were not using the wireless network. [59] On the other hand, if the neighbor downloads large files from the Internet, or engages in file-sharing or media-streaming, the neighbor will tax the router's resources. [60] A Wi-Fi operator would notice a delay in the transmission speed. [61] Nevertheless, even where there is such a delay, there is no immediate indication to the Wi-Fi operator that the neighbor has accessed the [1234] wireless network. [62] The Wi-Fi operator would experience a transmission delay, but would not know the source of that delay. [63]

Wi-Fi operators can prevent joyriding by simply setting up a password that users must provide to access the wireless network. [64] However, most Wi-Fi operators do not invoke such security measures. [65] It is therefore likely that most instances of joyriding do not consist of "hacking" into a password-protected wireless network. For the purposes of this Article, "joyriding" refers to the unauthorized access of a wireless network, which is not password protected, for the sole purpose of engaging in Internet activity.

III. THE ELEMENTS OF TRESPASS TO CHATTEL APPLIED TO WI-FI JOYRIDING

This Part examines whether the joyriding neighbor's conduct gives rise to a claim of trespass to chattel. [66] A trespass to chattel lies where [1235] an actor intentionally dispossesses another of a chattel, or alternatively, uses or intermeddles with a chattel in possession of another. [67] Section III.A considers the possible chattel on which the joyriding neighbor allegedly trespasses. Section III.B analyzes whether the neighbor's conduct is trespassory in nature. A discussion of the possible defenses to trespass to chattel follows in Part IV.

A. The Chattel

Trespass to chattel requires that a chattel exist. [68] If the joyriding neighbor commits a trespass to chattel against the Wi-Fi operator, the Wi-Fi operator must own a "thing" on which a trespass can be committed. [69] At first glance, the "thing" to be considered in the trespass analysis seems to be the wireless network. [70] As discussed below, however, a wireless network does not possess characteristics of property which are necessary for ownership. Therefore the "thing" to be considered in the trespass analysis should not be the wireless network; instead, for reasons discussed below, the "thing" should be the Wi-Fi router.

The view that the wireless network is a chattel against which a trespass may be committed essentially posits that a Wi-Fi operator should be rewarded for laboring to create the network. [71] It is the Wi-Fi operator who purchases and installs a router that makes the network even possible. On the basis that laborers should hold property rights in the fruits of their labors, the Wi-Fi operator arguably should own the radio signals that the Wi-Fi router transmits. [72] The Wi-Fi operator is, in effect, the creator of the transmission. As the creator, [1236] the Wi-Fi operator seems to hold property rights over the creation - the wireless network, or in other words, the Wi-Fi radio-signal transmission. [73]

This argument is unpersuasive. Although a person may expend great labor to produce an outcome, that outcome does not necessarily produce a thing to which property rights may attach. [74] Property requires exclusivity. [75] Regardless of whether the subject of property is tangible or not, that subject must be capable of exclusive control and possession. [76] The wireless network is not capable of being exclusively controlled or possessed because it includes radio signals. [77] Radio signals cannot be contained within a geographic boundary. [78] Their only boundary is their bandwidth frequencies, and those frequencies are unlicensed, meaning that the government

has permitted any person to transmit signals over the frequencies. [79] Coterminal use of the frequencies is therefore permissible, which could produce interference [1237] between competing signals. [80] A Wi-Fi operator cannot exclude another person from using a frequency, meaning that a Wi-Fi operator cannot exclude another person from interfering with Wi-Fi radio signals. [81] In short, Wi-Fi radio signals do not admit exclusivity, so they should not be viewed as property. [82]

It should be noted that the capability to password protect a wireless network does not satisfy the exclusivity requirement of property. Although a Wi-Fi operator can password protect the wireless network against unwanted use, the Wi-Fi operator cannot preclude another person from interfering with the Wi-Fi radio signals. [83] The fact that interference is possible, and moreover permissible, [84] demonstrates that a Wi-Fi operator is unable to exercise exclusive control and possession over the Wi-Fi radio signals. The password protects another person from interpreting Wi-Fi signals, but not from interfering with the signals. Password protection does not imply that the operator can exclude others from interfering with the Wi-Fi radio signals. They are not property.

Although the radio signals composing the network are not property, a physical piece of equipment that makes possible the network indisputably is. The router - the network component through which Wi-Fi radio signals are transmitted - is property. [85] Unlike radio signals which are incapable of exclusive control and possession, the Wi-Fi router is continually in the control and possession of the Wi-Fi operator. Even during the neighbor's joyriding, the router remains physically with the Wi-Fi operator. The Wi-Fi operator therefore holds an undisputable property interest in the router. The question of trespass is thus whether the neighbor's use of the router constitutes a violation of the Wi-Fi operator's property rights in the router.

[1238]

B. The Trespass

"The law hath not been dead, though it hath slept." [86] The tort of trespass to chattel has lain dormant for years, having been employed in times past to remedy farmers for injuries that were intentionally inflicted on sheep and cattle. [87] Recently, however, the tort has been revived to deal with troubles in cyberspace. [88] Courts have resurrected the doctrine to prohibit the sending of unsolicited mass e-mails and the searching of websites by robotic software. [89] Trespass to chattel has served as a legal means for controlling traffic in cyberspace. Still undetermined is the question of whether the tort's application to the ontology of cyberspace encompasses Wi-Fi joyriding. [90]

An actionable trespass to chattel occurs when an actor intentionally either dispossesses another of a chattel, or alternatively, uses or "intermeddles" with the chattel while it is in the possession of another. [91] In the context of Wi-Fi joyriding, the neighbor does not physically dispossess the Wi-Fi operator of the router. The neighbor uses the router while it remains in the physical possession of the Wi-Fi operator. Accordingly, the question of whether the neighbor trespasses on the router involves an examination of whether the neighbor has intentionally used or "intermeddled" with the router.

To use or intermeddle with a chattel, an actor must bring about physical contact with the chattel. [92] Physical contact may occur if the actor physically touches the chattel, or if the actor causes something else to touch the chattel. [93] A touching results in intermeddling. [94] Yet not all instances of intermeddling give rise to liability for trespass to chattel. [95] Liability arises only if the intermeddling causes harm. [96] Harm is manifest by an impairment of the chattel's condition, quality, [1239] or value. [97] In the absence of any of these conditions, the intermeddling is harmless, and thereby not actionable. [98]

The following three subsections examine whether Wi-Fi joyriding satisfies these requirements for trespass to chattel. Subsection III.B.1 examines whether the neighbor's use of the Wi-Fi operator's router results in physical contact sufficient to constitute intermeddling. Subsection III.B.2 examines whether the alleged contact results in harm. Subsection III.B.3 examines whether the neighbor's use of the router is intentional.

1. Physical Contact

Perhaps most intriguing about the Wi-Fi trespass argument is the issue regarding whether a trespass is possible even though the neighbor never causes a material object to physically contact the Wi-Fi router. [99] The argument for trespass relies on the premise that the neighbor causes physical contact with the router when the neighbor transmits electronic signals through the router in order to access the Internet. [100] Although that premise has not yet been considered by any court, courts have considered whether electronic signals satisfy the physical-contact element in the context of Internet users sending e-mail and accessing information on websites. [101] As discussed below, these e-mail and website cases suggest that Wi-Fi joyriding satisfies the physical-contact element of trespass to chattel.

a. Jurisprudence Dealing with Physical Contact in Cyberspace

Amidst public frustration with unsolicited mass e-mails, courts have held that transmitting such e-mails constitutes a trespass to chattel. [102] The first instance occurred in *CompuServe, Inc. v. Cyber Promotions, Inc.* [103] There, the defendants sent unsolicited mass e- [1240] mails to subscribers of an ISP, CompuServe. [104] The federal district court held that the defendants had trespassed on CompuServe's computer equipment, finding that the defendants had "intermeddled" with the equipment. [105] In so holding, the court specifically held that the electronic signals which the defendants had generated in order to send the e-mail through CompuServe's computer equipment resulted in physical contact. [106]

Soon after *CompuServe*, trespass to chattel was routinely deployed to cease the practice of mass e-mailing. [107] For instance, in *America Online, Inc. v. IMS*, [108] a federal district court relied exclusively on *CompuServe* to find that the defendant had trespassed on an ISP's property. As in *CompuServe*, the IMS court held that the electronic signals that the defendants had sent as e-mails through the plaintiff's computer equipment were sufficient to constitute a "contact" for purposes of establishing trespassory intermeddling. [109] Following *IMS*, the same federal district court faced the same issue in *America Online, Inc. v. LCGM, Inc.* [110] Without hesitation, the LCGM court declared that "the transmission of electrical signals through a computer network is sufficiently 'physical' contact to constitute a trespass to property." [111] Thus, *CompuServe*'s substantive alteration of an age-old tort principle was readily accepted by courts. [112] Its rationale continues to be deployed against defendants who send unsolicited mass e-mails over the Internet. [113]

Following the lead of these trespass-by-e-mail cases, courts applied the doctrine of trespass to chattel as a means for precluding Internet users from engaging automated software to collect data from websites. [114] [1241] In *eBay, Inc. v. Bidder's Edge, Inc.*, [115] the defendant, Bidder's Edge, executed a computer program, otherwise known as a "bot," to search and retrieve data from the website of the plaintiff, eBay. [116] The court held that the electronic signals sent by Bidder's Edge through the bot to eBay's server were "sufficiently tangible to support a trespass cause of action." [117] Electronic signals satisfied the physical-contact requirement. [118] Subsequently, in *Register.com, Inc. v. Verio, Inc.*, [119] another federal district court ruled that searching websites by using an automated software bot constituted a trespass to chattel. [120] The court did not even offer an explanation for the fact that physical contact had occurred. [121] The court's failure to address this point suggests that it was so well established that it did not merit discussion.

These cases adopt a rationale that electronic signals which interact with physical components of computer equipment satisfy the physical-contact requirement for trespass. [122] Notable is the fact that physical contact has been found in situations where the computer equipment facilitates Internet communication. It appears that the intangible nature of the Internet affects the physical-contact requirement of trespass: where the alleged trespass occurs on the Internet, the contact need not be with a physical object, but rather can be with an electronic wave. Also notable is the fact that in cases where courts have held that a trespass to chattel did not occur on the Internet, the courts have not taken issue with the principle that electronic signals satisfy the physical-contact requirement. [123] Cyberspace jurisprudence thus appears to establish that electronic signals that contact a computer component which facilitates Internet communication is sufficient to satisfy the physical-contact requirement of trespass to chattel. [124]

[1242] Applying this principle to the Wi-Fi context reveals that the joyriding neighbor who sends electronic signals through the Wi-Fi router is causing physical contact with the router. A Wi-Fi router is a physical component of computer equipment that facilitates Internet communication. [125] The reasoning of the cases described above implies that the electronic signals that contact the router constitute physical contact sufficient to support a finding of intermeddling.

b. Criticism of Physical Contact in Cyberspace

The view that physical contact occurs when an electronic signal contacts a physical object is not without criticism. [126] The evident flaw with the view is that a Wi-Fi electronic signal is not a material object. [127] It is a wave that travels through air. [128] If an electromagnetic wave is capable of causing physical contact with a chattel, then other forms of waves would be capable of causing physical contact. For example, physical contact would result when a person directs an air fan to blow air onto another's flag, yet this does not seem to be a tenable example of trespassory physical contact. Consequently, the view that Wi-Fi signals satisfy the physical-contact element of trespass to chattel opens the door to situations where it would seem ridiculous to find trespassory intermeddling.

One commentator has raised a similar criticism of the physical-contact element in the context of Internet trespass cases. [129] Trespassory physical contact over the Internet, according to the commentator, gives rise to ridiculous implications. [130] Unwanted telephone callers send electronic signals to another's telephone, so they would commit a trespass to chattel; the same could be said of people who transmit facsimiles or television broadcasts. [131] Electronic signals from baby monitors which interfere with the operation of cordless telephones would also result in trespass. Such bizarre results would seem to preclude the conclusion that an electronic signal satisfies the physical-contact requirement of trespass to chattel. [132]

These criticisms would be well grounded if intermeddling were the only element of an actionable trespass to chattel. Indeed, nearly every device capable of producing airwaves or electronic signals would constitute a means for committing a trespass to chattel. Such an outcome cannot be. And it is not. As discussed above, trespassory intermeddling [1243] requires that the physical contact cause actionable harm, and that the intermeddling be intentional. [133] With respect to harm, the seemingly "ridiculous" examples of airwaves and electronic signals causing physical contact lack this necessary element. The lack of harm in the airwave example is obvious: blowing airwaves onto a flag does not damage the flag. However, if a person directed a powerful air fan toward a lightweight vase that was precariously standing upright, and in so doing caused the vase to blow over and break, then the airwaves would be the means of committing actionable physical contact. The same is true of electronic signals. A telephone caller causes electronic signals to contact another's telephone, but the signals do not result in any damage to the telephone that is contacted. [134] By contrast, if a person were to cause a power surge to short a cordless telephone so that it was no longer operable, then the contact by the electronic signals would have resulted in a trespass. An action for trespass lies only if physical touching - by physical object, by airwave, or by electronic signal - results in harm to the chattel. [135]

Intentionality must also exist for an intermeddling to be tortious. [136] According to the Restatement, trespass to chattel does not lie unless the actor acts "for the purpose of using or otherwise intermeddling with a chattel or with knowledge that such an intermeddling will, to a substantial certainty, result from the act." [137] In other words, an actor must intend to contact the chattel at issue for trespass to lie. [138] Most instances where an electronic device interferes with the performance of another electronic device are not likely intended. For instance, parents do not usually intend for their baby monitors to interfere with nearby cordless phones. An action for trespass would [1244] not lie. [139] On the other hand, if a person intentionally employed a radio jammer to interfere with the signal of a cordless phone so that it was inoperable, then a trespass would lie. Whereas the concerned parent would never face liability for trespassing by baby monitor, the radio jammer would. Wireless radio interference is usually unintentional, preventing otherwise ridiculous instances of trespass.

In sum, the view that electronic signals and airwaves can be the means of committing actionable physical contact appears sound. The ridiculous examples that the above criticisms raise would never result in liability for trespass. Just as patting another's horse or accidentally tripping on another's cat does not result in actionable trespass, [140] neither does blowing air on a flag, placing a telephone call, or interfering with a baby monitor. Trespassory liability requires harm and intentional conduct. [141] In conjunction with those elements, electronic signals and airwaves can constitute means for trespassing on a chattel.

2. Harm

a. Two Actionable Harms

As most wireless electronic signals do not result in actionable harm, an issue arises as to whether the neighbor who joyrides on the wireless network causes harm to the router of the Wi-Fi operator. To satisfy the harm requirement, the physical contact must impair the chattel's condition, quality, or value, or alternatively, the contact must result in the owner being deprived of the chattel's use for a substantial time period. [142] Impairment must be actual rather than merely possible. [143] In the Wi-Fi context, two harms are possible: (i) decreasing router performance for the Wi-Fi operator; and (ii) transmitting computer viruses through the router to the Wi-Fi operator's computer. [144] [1245] As discussed below, these consequences of joyriding should demonstrate sufficient harm to impose liability for trespass.

The first harm occurs where the Wi-Fi operator experiences a delay while accessing the Internet through the router. When the neighbor accesses the Internet through the Wi-Fi operator's router, the neighbor consumes resources of the Wi-Fi router. [145] For example, if the neighbor were to download large media files from the Internet, the neighbor would decrease the speed at which the router transfers data to the Wi-Fi operator. [146] Similarly, if the neighbor were to engage in peer-to-peer file sharing over the Internet, the neighbor would compromise router performance. [147] Hence, when the neighbor intermeddles with the Wi-Fi operator's router, the neighbor could harm the Wi-Fi operator's ability to optimally use the router. [148] A router that transmits data slower than it otherwise could is less valuable to the Wi-Fi operator. The first harm appears to result in an impairment of the router's value.

The second harm occurs where the Wi-Fi operator receives a computer virus from the neighbor's computer. [149] By joyriding, a neighbor [1246] can unknowingly subject all other computers within the wireless network to a virus. [150] This is possible because all computers within the same wireless local area network indiscriminately share data through the Wi-Fi router. [151] Consequently, the router becomes a device for disseminating viruses from the neighbor's computer to the Wi-Fi operator's computer. The neighbor's conduct transforms the router from a valuable conduit for Internet access to a noxious chamber of virus diffusion. [152] When the neighbor transmits electronic signals containing a virus through the Wi-Fi operator's router, the value of the router decreases. The second harm thus results in an impairment of the router's value. [153]

It could be argued that trespass to chattel does not lie because neither of these alleged harms actually impair the physical condition of the router. The Restatement provides that in most instances, actionable impairment of a chattel must result from some impairment of the physical condition of the chattel. [154] With respect to the first harm, the delay that the Wi-Fi operator may notice while the neighbor is joyriding does not imply that the router is physically dysfunctional. On the contrary, the router functions exactly as it should: it splits its resources between the computers connected to the wireless network. [155] [1247] A delay in data transmission may result from the neighbor's use of the router, but that router is performing as optimally efficient as it is capable of performing. [156] There is no physical impairment. With respect to the second harm, disseminating computer viruses through a router does not damage the physical condition of the router. [157] The viruses pass through the router, but they do not actually harm the functionality of the router. [158] During and after the transmission of a computer virus through a router, the router performs just as it did prior to the virus transmission. It continues to send and receive data in an efficient manner. Thus, neither delaying a Wi-Fi operator's data transmission nor transmitting a virus through the router results in physical impairment of the router.

Admittedly, the neighbor's conduct does not physically impair the router. This fact, however, does not imply that the neighbor has not committed a trespass. [159] A harmful trespass to chattel may occur when an actor temporarily deprives another of the ability to use a chattel, even where the chattel is not physically impaired or where the actor does not physically dispossess the chattel from the owner. [160] For example, locking a car owner's keys in the car deprives the owner of the car's use, although

the car owner is not physically dispossessed of the car. Liability for such deprivation of use requires that the time period of deprivation be so substantial that it is possible to estimate [1248] the loss caused by that deprivation. [161] In the car example, if the car owner were deprived of using the car for a mere hour, trespass to chattel would lie according to the Restatement. [162]

The two harms that could result from the neighbor's intermeddling with the router appear to deprive the Wi-Fi operator of the router's use in a manner sufficient to impose trespassory liability. The delay that the Wi-Fi operator experiences because of the neighbor's joyriding demonstrates that the Wi-Fi operator is unable to use the full capacity of the router. Assuming that this delay occurs for a sufficient time period, e.g., an hour, [163] the deprivation of use would give rise to a trespass. Similarly, a computer virus that the Wi-Fi operator receives through the router demonstrates that the Wi-Fi operator is unable to use the router without inhibition, i.e., connecting to the Internet without receiving viruses from other computers within the wireless network. The Wi-Fi operator is deprived of realizing full use of the router. As infinitesimally short as the time period is in which the virus passes through a router, the time period would nevertheless be of a sufficient duration to be actionable because the harm would be calculable. [164] Thus, the Wi-Fi operator cannot make full use of the router where the two harms occur.

That the Wi-Fi operator can still make a partial use of the router while the neighbor is joyriding should not affect the conclusion that actionable harm occurs. In effect, the two possible harms represent trespasses on two "sticks" within the Wi-Fi operator's "bundle of sticks." [165] Although the Wi-Fi operator can exercise other property uses in the router, the Wi-Fi operator cannot exercise every use. Disabling a chattel owner's ability to exercise only some uses over the chattel - rather than all uses - results in a trespass to chattel, whereas disabling a chattel owner's ability to exercise all rights results in conversion. [166] It is this distinction between disabling a portion of property rights in a chattel and disabling all property rights in a chattel that gives rise to the two different causes of action. [167] As one commentator [1249] notes, trespass to chattel is the little brother to conversion. [168] Hence, the fact that the Wi-Fi operator is still able to exercise some property rights in the router does not detract from the argument that a trespass lies. [169] The fact is consistent with the doctrine of trespass to chattel. [170]

b. Harmless Intermeddling with the Router

The two harms described above - delay in data transmission and dissemination of viruses - appear to satisfy the requirement for harm under the tort of trespass to chattel. [171] But a neighbor can joyride without either of these harms occurring. The Wi-Fi operator would not notice any delay in the speed of data transmission if the neighbor uses the Wi-Fi router merely to view websites or to check e-mail. [172] Nor would the router be a means for transmitting viruses if the neighbor's computer is not infected with one. Seemingly harmless intermeddling could therefore result from joyriding. [173]

Despite the doctrine that harmless intermeddling does not produce an actionable trespass to chattel, [174] a strong argument can be made that an exception to this general doctrine should exist where the intermeddling occurs in cyberspace. Support for such an exception arises in caselaw. [175] In the context of cyberspace, courts have not always [1250] adhered to the requirement that there must be actual harm for an actionable trespass to chattel to lie. [176] Bidder's Edge is a good example. [177] There, the bot device that Bidder's Edge used to search eBay's website consumed approximately one percent of eBay's server capacity. [178] Consequently, the bot did not detract from eBay's ability to meet the needs of all other Internet users who accessed its website. [179] The court, however, held that Bidder's Edge caused eBay harm because the bot "consumed at least a portion of [eBay's] bandwidth and server capacity." [180] Recognizing that the level of bandwidth that Bidder's Edge consumed did not actually pose any harm to eBay, the court reasoned that if that activity were permissible, then the activity could increase, and in the aggregate, the activity could harm eBay. [181] While admitting that there was no actual harm, the court found the harm requirement of trespass to chattel to be satisfied. [182]

Bidder's Edge does not stand alone in judicial softening of the harm requirement. In Register.com the court contemplated the same facts as those present in Bidder's Edge. [183] As in Bidder's Edge, the Register.com court found an actionable harm based on the defendant's use of automated software that searched a website. [184] The court opined that the "possibility" of harm to the plaintiff's server capacity was sufficient to satisfy the harm requirement under trespass to chattel. [185] Similarly, in CompuServe, the court held that the mass e-mail that the defendants had sent through the ISP produced actionable harm because the e-mail placed a "demand" on disk space and processing power, which resources could have otherwise been available for [1251] ISP customers. [186] That demand, however, did not detract from the capability of the ISP's computer equipment to function properly. [187] Indeed, any single e-mail results in a demand of disk space and processing power. [188] The mass e-mails did not deter the ISP's ability to facilitate Internet traffic; instead, the e-mails merely invoked that ability. [189]

These cases suggest that in the context of determining whether electronic trespass exists on the Internet, the harm necessary for an actionable trespass need only be minimal in nature. Courts have looked to the potential for harm, rather than actual harm, in deciding whether the harm element is satisfied in cyberspace. [190] An electronic signal is harmful when it could affect the performance of the physical object at issue if the signal were duplicated in the aggregate. [191]

One case that implicitly supports this interpretation of these cases is Intel Corp. v. Hamidi. [192] There, the California Supreme Court considered whether a trespass to chattel occurred when the defendant sent e-mails critical of his former employer, Intel, to current Intel employees. [193] The court held that the tort did not lie because the alleged harm stemmed from the content of the e-mails, rather than an injury to the functionality of Intel's computer system. [194] In its analysis, the court distinguished Bidder's Edge, Register.com, and CompuServe on the grounds that those cases dealt with either actual or "threatened" harm, whereas the defendant's e-mails neither actually harmed nor threatened to harm his employer's computer system. [195] The Hamidi decision therefore implicitly endorses the potential-for-harm rationale set forth in the above cases. [196]

Also notable in Hamidi is the fact that Intel argued that the e-mails caused harm in the form of economic damage. [197] The Intel employees, Intel alleged, were distracted by the content of the e-mails, [1252] causing Intel to incur loss of productivity. [198] The Hamidi court rejected this argument, holding that economic damages did not satisfy the harm requirement of trespass to chattel. [199] The tort required the harm to be directly to the chattel. [200] Thus, consequential business-related damages appear to be neither sufficient nor necessary for trespass to chattel to lie in the context of sending electronic signals over the Internet. [201]

According to this recent Internet jurisprudence, the radio signals that a joyriding neighbor sends to a Wi-Fi operator's router appear to constitute trespassory harm. As Bidder's Edge, Register.com, and CompuServe suggest, the potential for physical harm that an electronic signal poses to computer equipment appears sufficient to satisfy the harm requirement. [202] The fact that the harm does not cause consequential economic damage to the owner of the computer equipment should not, according to Hamidi, affect the trespassory analysis. [203] These general principles imply that the electronic signal which the neighbor causes to contact the Wi-Fi operator's router is sufficient to constitute trespassory harm. Although the neighbor's signal may not drain the router's capacity, if duplicated in the aggregate the signals would. [204]

Tellingly, courts have remained silent as to why they have softened the harm requirement for a trespass to chattel arising in cyberspace. [205] Their silence suggests that policy concerns outweigh the value of an antiquated tort doctrine. [206] At the outset of the Internet, uncertainty as to how the law would treat the new electronic medium threatened to hamper its commercial viability. [207] Faced with a promising new medium of exchange, and likely noting its relatively infantile stage, courts delivered the needed certainty. Courts provided market participants certainty that their Internet investments were [1253] well protected, and they did so even before any harm occurred. [208] Confidence in the new intangible, commercial medium could not be sacrificed at the expense of upholding a doctrine that was crafted for problems arising in the disparate realm of the physical. The policy of promoting and protecting valuable benefits of the Internet prevailed over a principle established for a wholly distinct ontology.

This policy of liberally protecting Internet investors strengthens the argument that a joyriding neighbor has acted tortiously. Because the neighbor can access a wireless network at no cost, the neighbor is neither likely to purchase a Wi-Fi router nor likely to purchase the services of an ISP. It seems likely that at least some joyriding neighbors value the Wi-Fi connection at a level equal to or greater than the cost of ISP services or of a Wi-Fi router. [209] Assuming that this is true, these joyriding neighbors would purchase ISP services and Wi-Fi routers if they were not provided the opportunity to access the Internet through Wi-Fi operators' networks. ISPs and

manufacturers of Wi-Fi routers are therefore not realizing a complete economic return on their investment in Internet technology. [210] Prohibiting joyriding would ensure that they are rewarded for their investment.

The upshot of this discussion about the seemingly harmless nature of Wi-Fi joyriding is that the joyriding does result in a harm, but on a macro level. Judicial holdings dealing with equipment that facilitates Internet activity seem to indicate that if the conduct at issue would produce harm were it duplicated in the aggregate, then the harm requirement is satisfied. [211] Those holdings also implicitly indicate that protecting participants of Internet-based technology is sufficient reason to find actionable harm where a single instance of intermeddling could produce harm if duplicated en masse. [212] In short, there appears to be room in cyberspace to carve out an exception to the requirement that the chattel owner experience actual harm. And Wi-Fi technology [1254] should be a part of that cyberspace exception. Seemingly harmless intermeddling should be actionable.

3. Intent

The joyriding neighbor appears to satisfy the intentionality requirement of trespass to chattel. To commit a trespass to chattel, an actor must intend to commit the intermeddling contact. [213] This means that the joyriding neighbor must intend to use another person's router. [214] The presence of this intent is apparent. In accessing the router, the neighbor chooses a wireless network through which his or her wireless network adapter can interface. [215] By selecting the Wi-Fi operator's network from a computer prompt, the neighbor affirmatively demonstrates an intent to use another person's router. The neighbor's intentional selection of the Wi-Fi operator's wireless connection demonstrates an intent to intermeddle with the router.

Two further points are worth noting about the joyriding neighbor's intent. [216] First, the fact that the neighbor does not intend to harm the Wi-Fi operator does not affect the intent analysis. An actor need not intend to commit the harm that results from an intermeddling; the intent requirement is satisfied even where the actor acts under a mistake of fact. [217] A harmful intermeddling is not excused on the basis that the actor believed that the intermeddling would not be harmful. [218] Accordingly, the neighbor's intent to access the Internet through the router is sufficient to satisfy the intent requirement. That the neighbor does not intend to slow down the data transmission for the Wi-Fi operator, to spread a virus to the Wi-Fi operator, or to impede the market for ISP service should not affect whether the neighbor satisfies the intent requirement. [219]

[1255] Second, assuming that the neighbor does not know the identity of the Wi-Fi operator, such that the neighbor knows only that the Wi-Fi router belongs to some other person, the intent requirement is still satisfied. Intermeddling is present even if the actor does not know the identity of the chattel owner. [220] Throwing a baseball at a car satisfies the intent requirement of trespass to chattel, even where the car owner is unknown to the thrower. Likewise, accessing the Internet through a wireless network that does not belong to the neighbor satisfies the intent requirement, even where the identity of the Wi-Fi operator is unknown to the neighbor. It is sufficient that the joyriding neighbor knows that the Wi-Fi connection is not his or her own.

IV. DEFENSES OF TRESPASS TO CHATTEL APPLIED TO WI-FI JOYRIDING

A joyriding neighbor could argue two defenses to the trespass to chattel claim. The first is that the Wi-Fi operator has consented to the joyriding by failing to password protect the router from unauthorized use. [221] The second is that joyriding constitutes a permissible means for the neighbor to abate a nuisance that the Wi-Fi operator creates - hogging the wireless spectra. [222] Neither defense should prevail. Each is discussed below.

A. The Wi-Fi Operator's Seeming Consent to Joyriding

A joyriding neighbor could argue that joyriding is permissible because the Wi-Fi operator has failed to implement security measures which would preclude the neighbor from accessing the router. A person who consents to otherwise tortious conduct cannot recover against the actor. [223] Consent may be manifest by action or inaction, and need not be communicated to the actor. [224] When a person's silence would be reasonably understood as intended to indicate consent, that silence is a manifestation of apparent consent. [225]

[1256] The neighbor's consent argument is based solely on the fact that the Wi-Fi operator fails to implement a password so that others cannot access the Internet through the router. The argument effectively implies that anyone should be permitted to access a wireless network unless the Wi-Fi operator institutes security measures. The argument draws support from cyberspace jurisprudence. [226] In *EF Cultural Travel BV v. Zefer Corp.*, [227] the First Circuit considered whether a website owner had provided consent for the defendant to use automated software to search its website. [228] The court concluded that because the website owner had not expressly restricted the use of the website, the owner had implicitly consented to the defendant's conduct. [229] In dicta, the court commented that a lack of consent can be manifest by the presence of password protection. [230]

Other courts have considered the issue of consent. In *CompuServe*, the court opined that the ISP provided "tacit" consent for anyone on the Internet to send e-mail to its subscribers, but that the ISP had affirmatively revoked its consent to the defendants. [231] The basis for this finding of "tacit" consent was that the ISP had created a system for allowing anyone on the Internet to e-mail its subscribers. [232] In other words, consent was based on the fact that the ISP system was designed for the purpose of allowing anyone on the Internet to send e-mails to subscribers. [233]

The Bidder's Edge court also opined on the doctrine of consent. [234] The court held that eBay had granted "conditional" consent to Internet users to access its website. [235] The consent was granted upon an express condition on its website stating that users were not to use robotic data-collection devices on its site. [236] In other words, a presumption of consent existed, and eBay acted to limit that presumption. [237] Restriction of website access was obtained by making a [1257] statement on the website, implicitly suggesting that a presumption of consent did exist. [238]

Relying on these cases, the joyriding neighbor could argue that the absence of any password protection by the Wi-Fi operator implies that the Wi-Fi operator consents to anyone using the router. Zefer seems to imply that the absence of password protection denotes consent to use property in cyberspace. [239] Further, like the ISP in *CompuServe*, a Wi-Fi operator creates a system specifically designed to allow anyone within its range to access the Internet. [240] Because the very function of the Wi-Fi connection is to provide any person within its physical range access to the Internet, that function arguably creates a presumption that the Wi-Fi operator consents to anyone accessing the Internet through the router. [241] Finally, just as the website owner in *Bidder's Edge* could easily restrict the presumption that anyone could access the owner's website, [242] the Wi-Fi operator can easily restrict the presumption that anyone can use the Wi-Fi operator's router: the Wi-Fi operator need merely set up a password. [243] By failing to implement a password, the Wi-Fi operator seems to assume the risk of Wi-Fi joyriding.

Despite these arguments in favor of construing the Wi-Fi operator's failure to implement a password as implicit consent for others to joyride, such a presumption should not exist. As an initial matter, Zefer's statement that a password denotes an absence of consent does not imply that an absence of a password denotes consent. [244] An analogy may illustrate the disconnect between these propositions. Consider a bicycle owner. If the owner locks the bicycle, the lock demonstrates that the owner does not consent to another person's use of the bicycle. But if the owner does not lock the bicycle, this does not imply that the owner consents to another's use of the bicycle. It is entirely possible that the bicycle owner does not lock the bicycle because the owner has trouble remembering combinations, or perhaps disdains spending time entering combinations to unlock property. Analogously, the absence of a password on a wireless network does not imply that the Wi-Fi operator consents to another's use of the router. That absence implies nothing more than the fact that the Wi-Fi operator chooses not to implement a password. Perhaps the Wi-Fi operator disdains having to spend time entering a password each time the operator [1258] accesses the Internet, or perhaps the owner simply has a bad memory for remembering passwords. Failure to install protective devices so that another cannot use property does not imply that a property owner consents to the use. Hence, Zefer's observation that the presence of a

password implies the absence of consent should not be construed as meaning that an absence of a password implies the presence of consent.

On a more substantive level, the cited cases should not be interpreted as suggesting that a Wi-Fi operator has consented to joyriding because none of the cited cases deal with wireless networks. The fact that the consent in the cited cases was manifest by ISPs and website owners distinguishes them from the context of wireless networks. [245] An ISP usually realizes economic benefit when Internet users make use of the ISP's services, including its e-mail service. [246] E-mail exchange increases demand for the ISP service. [247] Likewise, a website usually becomes more commercially valuable as more Internet users view the website. [248] In short, the commercial model for the Internet has developed such that the conduct of e-mailing ISP subscribers and viewing websites are activities that propagate economic benefits for ISPs and website owners. [249] For this reason, the presumption is sound that these property owners consent to otherwise trespassory contact in cyberspace.

The situation of a Wi-Fi operator is markedly different than that of an ISP or a website owner. A joyriding neighbor engages in free-riding parasitic behavior. Although the Wi-Fi operator may not necessarily be harmed by the behavior, the Wi-Fi operator does not stand to gain any economic benefit. In the absence of any possibility that the Wi-Fi operator could realize economic benefit from the neighbor accessing the Internet, the presumption that the owner has consented appears unjustified. Other than altruistic tendencies, there is no reason [1259] that a Wi-Fi operator would consent to joyriding. Presuming consent would be imposing a choice where the Wi-Fi operator was unaware of the conduct and preferred not to implement a password. In the Wi-Fi context, there is no reason to create a presumption of consent based on the absence of a password.

The absence of password protection also does not denote an assumption of risk that excuses the joyriding neighbor's conduct. It is true that by not implementing a password the Wi-Fi operator assumes the risk that a neighbor will joyride. But that fact does not excuse the neighbor's conduct. Assumption of risk is relevant in examining only a claim of negligence. [250] The inquiry at hand is one of intentional tort. [251] As much as a chattel owner may put at risk the safety of a chattel, if an actor commits an intentional trespass on the chattel without the owner's consent, the actor is still liable. [252] Assumption of risk is not a defense to intentional tort. [253] Consider a china-shop owner who invites a bull owner to shop at the china shop - with the bull. Unquestionably the china-shop owner assumes a great risk in extending that invitation. Yet if after walking into the china shop with the bull, the bull owner strikes the bull intending for the bull to destroy all the china, the bull owner is still liable for the resultant damage. That the china-shop owner places at risk all the china by allowing the bull to enter the shop is of no consequence. [254] The intentional act of the bull owner creates tortious liability. Similar to the china-shop owner, the Wi-Fi operator places at risk the router's use. [255] That risk is of no consequence because the joyriding neighbor intentionally acts to interfere with the Wi-Fi router. The intent is dispositive.

It should lastly be noted that the Wi-Fi operator's failure to password protect the network is not akin to establishing consent through [1260] silence. Silence or inaction can denote consent, but only where the chattel owner has knowledge of the actor using the chattel. [256] Silence or inaction does not denote consent where the actor is oblivious to the trespassory conduct. [257] Accordingly, failure to password protect a wireless network could possibly be viewed as consent through silence only if the Wi-Fi operator were aware of the conduct prior to choosing not to password protect the network. The Wi-Fi operator's inaction is not consent unless the Wi-Fi operator is aware of the tortious conduct. [258] But even then, a single oral objection to the use would preclude the possibility that the Wi-Fi operator consents where the Wi-Fi operator has not password protected the network. [259] Fences and locks are not necessary to show that a property owner does not consent to another's use of the property. [260] A simple, one-time oral communication should suffice.

B. The Joyriding Neighbor's Seeming Abatement to a Wi-Fi Nuisance

Another defense that the neighbor could argue is that joyriding is permissible under the abatement-of-nuisance doctrine. [261] The common law permits an actor to commit an act which would otherwise be a trespass to chattel when the act is committed for the purpose of abating a private nuisance that is caused by the chattel owner. [262] A private nuisance occurs where there is interference with a landowner's [1261] private use and enjoyment of land. [263] Abatement of the nuisance is permissible to the extent that the abatement is considered reasonable. [264] For instance, courts have considered it reasonable for a neighbor to cut tree branches which were overhanging into the airspace over the neighbor's land. [265]

The joyriding neighbor could argue that the Wi-Fi operator is causing a nuisance on the neighbor's property. There are a limited number of channels within the bandwidth frequencies on which Wi-Fi radio signals can exist. [266] By operating a wireless network, then, the Wi-Fi operator causes a shortage of channels on which the neighbor could operate a wireless network or other wireless device. The neighbor cannot set up his or her own wireless network because someone else is hogging the band. In other words, the neighbor cannot enjoy the use of the radio signals on the airspace over the land, so a nuisance seems arguably present.

After arguing that the Wi-Fi operator is causing a nuisance, the joyriding neighbor could further argue that a reasonable abatement of this nuisance would be to make use of the wireless network. By using the Wi-Fi operator's network, the neighbor abates the harm that the Wi-Fi operator has created. A shortage of bandwidth is of no concern to a neighbor seeking wireless Internet access if the neighbor can access the Internet through Wi-Fi radio signals that are already present in the airspace over the neighbor's land. Thus, the neighbor could argue that the otherwise tortious conduct of joyriding is excused based on the neighbor's abatement of the Wi-Fi operator's nuisance. [267]

This abatement-of-nuisance argument would not likely succeed. To begin with, nuisance claims relating to radio-frequency interference are preempted by the Federal Communications Act ("FCA"). [268] The FCA contains no provision that would prohibit a person from using [1262] all possible frequencies on an unlicensed bandwidth. [269] It would not likely apply. [270] Because preemption precludes the neighbor from raising a nuisance claim, and because the FCA does not likely apply in that situation, the neighbor cannot likely raise this nuisance-abatement argument.

Assuming arguendo that the neighbor could raise the nuisance-abatement argument, it would be highly unusual that abatement would be permissible. Abatement is permissible only in situations of extreme or urgent necessity. [271] The complained-of nuisance must actually exist. [272] In the Wi-Fi context, then, abatement would be permissible only if the Wi-Fi operator were causing a shortage of channels on the unlicensed frequencies, and only if the neighbor actually unsuccessfully attempted to access the Internet using his or her own Wi-Fi equipment and ISP. [273] This situation is highly unlikely. [274] As an initial matter, two wireless networks are capable of coexisting within the same close proximity. [275] Crowding out a wireless network would occur only if multiple other wireless devices were also in operation in the same close proximity. [276] The circumstance of close proximity suggests that those other wireless devices crowding out the neighbor's wireless network would likely belong to the neighbor. If the neighbor need merely stop using his or her microwave oven to operate the wireless network, the complained-of nuisance would not appear to be "extreme." [277] Abatement would not be permissible. [278]

[1263] Even more important in the abatement analysis is the fact that joyriding is not usually the result of the posited circumstances. Joyriding does not usually occur after a neighbor has subscribed to ISP services, has purchased a Wi-Fi router, and then has unsuccessfully attempted to connect to the ISP using that Wi-Fi router. Neighbors do not joyride because they are unsuccessful at operating their own Wi-Fi connection; they joyride to avoid paying ISP fees. The facts necessary to support a nuisance-abatement argument are simply implausible. [279]

V. CONCLUSION

The seemingly harmless conduct of accessing the Internet through another's wireless network without authorization should be deemed tortious. Joyriding should result in an actionable trespass to chattel. A joyriding neighbor appears to trespass on the Wi-Fi operator's router. [280] When the neighbor sends electronic signals through the router to access the Internet, those signals produce a physical effect on the router that is sufficient to be deemed trespassory physical conduct. [281] The neighbor intentionally causes this contact, thereby satisfying the intentionality requirement for trespass. [282] Harm may also be present. [283] The Wi-Fi operator may experience delayed Internet transmission or receive viruses from the joyriding neighbor. [284] Yet even if neither of these harms are present, a strong argument exists

that the joyriding neighbor should still be liable. [285 ±] Recent Internet jurisprudence suggests that using another's computer equipment to access the Internet results in a trespass to chattel, regardless of whether that access results in actual harm. [286 ±] In an effort to thwart the negative externality that joyriding causes ISPs and manufacturers [1264] of Wi-Fi routers, courts would likely view the joyriding neighbor's conduct as tortious. [287 ±]

A joyriding neighbor would not likely prevail in arguing defenses against the trespass claim. [288 ±] One arguable defense is that the Wi-Fi operator implicitly consents to the neighbor's conduct when the Wi-Fi operator fails to implement security measures such as a password. [289 ±] Yet the fact that a Wi-Fi operator may not implement a password to protect access to the network should not be interpreted as consent to the neighbor's conduct. [290 ±] The Wi-Fi operator's failure to implement password protections is akin to any physical property owner failing to secure his or her property with a lock. [291 ±] Failure to secure property does not denote consent. [292 ±] Nor does the fact that the Wi-Fi operator places the network at risk of a neighbor accessing it imply that the neighbor's act is excused. [293 ±] Assumption of risk is no defense to an intentional tort. [294 ±] It is also noteworthy that the Wi-Fi operator has no economic incentive to allow the neighbor access to the network. [295 ±] In the absence of an economic benefit for the Wi-Fi operator, there is no reason to presume that the Wi-Fi operator would condone joyriding. [296 ±]

Another arguable defense is that joyriding is a permissible abatement of an actionable nuisance. [297 ±] That nuisance arguably consists of the detriment that the wireless network causes to the neighbor's capability of setting up his or her own wireless network. [298 ±] This argument would not likely succeed. [299 ±] Nuisance claims arising from radio frequency interference are preempted by federal law under the FCA, and the FCA does not prohibit the interference that Wi-Fi radio signals might cause on unlicensed frequencies. [300 ±] Moreover, even if the FCA did not preempt nuisance claims, abatement is permissible only where harm actually occurs. [301 ±] Actual harm would occur only if the joyriding neighbor had first attempted to access the Internet through his or her own Wi-Fi connection, a situation which appears unlikely. [302 ±] The [1265] joyriding neighbor would not likely prevail in arguing a defense to trespass to chattel.

Thus, Wi-Fi technology appears to introduce a new stick into the bundle of sticks that a Wi-Fi operator holds over physical property. The Wi-Fi operator should be able to control the electronic signals that are directed through his or her router. Likely an owner of an umbrella, an automobile, or a football could not preclude another person from causing electronic signals to contact their respective property. Trespass to chattel in cyberspace thereby signifies a new sort of property right, a right which emerged due to the value that the physical property has brought to the virtual world. A Wi-Fi operator should hold a unique property right in the router because of the router's capability of facilitating communication in cyberspace. For its virtual value, a physical trespass to chattel should lie.

Copyright (c) 2006 University of Nebraska

Nebraska Law Review

Footnotes

[1] See Wi-Fi Alliance, The How and Why of Wi-Fi, <http://www.wi-fi.org/OpenSection/why/Wi-Fi.asp?TID=2#Wi-Fi Connects You Anywhere> (last visited May 15, 2006) (hereinafter *How and Why of Wi-Fi*) (describing advantages of Wi-Fi technology).

[2] See Benjamin D. Kern, Whacking, Joyriding and War-Driving: Roaming Use of Wi-Fi and the Law, 21 Santa Clara Computer & High Tech. L.J. 101, 103 (2004).

[3] *Id.* at 104.

[4] See, e.g., AT&T Residential: Internet Services, <http://www.consumer.att.com/plans/internet/> (last visited May 15, 2006) (offering monthly DSL service for \$ 29.95).

[5] See Kern, *supra* note 2, at 109.

[6] *Id.* at 104.

[7] Robert V. Hale II, Wi-Fi Liability: Potential Legal Risks in Accessing and Operating Wireless Internet, 21 Santa Clara Computer & High Tech. L.J. 543, 552 (2004); Matt Hines, Worried About Wi-Fi Security?, CNet News.com, Jan. 19, 2005, <http://news.cnn.com/Worried+about+Wi-Fi+Security/2100-73a7-3-5540969.html>.

[8] See Henry Kumagai, Mobile Technology Security Considerations, TechSoup.org, June 16, 2004, <http://www.techsoup.org/howto/articlepage.cfm?ArticleId=552&topicid=4> ("Two recently unleashed worms, Sasser and Kargo, infect one computer and then start looking for other networked computers close by to attack."). This Article contemplates only harms that usually occur unintentionally, such as the two described above. Nevertheless, other harms are possible. Those include accessing private information from a Wi-Fi operator's computer, such as credit-card or bank-account numbers. See Alex Leary, Wi-Fi Cloaks a New Breed of Intruder, St. Petersburg Times, July 4, 2005, at 1A, available at http://www.sptimes.com/2005/07/04/news/pl/State/Wi-Fi_cloaks_a_new_br.shtml. Another harm could occur where a joyriding neighbor causes a Wi-Fi operator to suffer disrepute. If a joyriding neighbor commits criminal acts over the Internet, those acts are traced back to the Wi-Fi operator. *Id.* This is so because each online connection produces an Internet Protocol ("IP") address, which is a unique numerical combination that can be traced to the physical place where the Internet connection is set up. *Id.* Hence, a joyriding neighbor's activities on the Internet can be traced back to the Wi-Fi operator. *Id.* In one instance, an e-mail containing death threats was sent to a school principal. *Id.* The IP address lead investigators to a dumbfounded family that had been operating a wireless Internet connection. *Id.* As it turned out, a neighborhood boy had tapped into their wireless network and sent the e-mail. *Id.*

[9] See Hale, *supra* note 7, at 547; Kern, *supra* note 2, at 104; Steve Hargreaves, Stealing Your Neighbor's Net, Money, Aug. 10, 2005, at 21, available at http://money.cnn.com/2005/08/08/technology/personaltech/internet_piracy/index.htm?cnn=yes (opining that Internet joyriding is becoming a common phenomenon); Leary, *supra* note 8, at 1A (commenting that experts believe that scores of joyriding incidents occur undetected, and that many people do not take the time to secure their wireless Internet connections).

[10] See Hale, *supra* note 7, at 547 (reporting that sixty-seven percent of wireless users do not implement security measures); Kern, *supra* note 2, at 109 ("A roaming Wi-Fi user obtains broadband Internet access service, a valuable service, without paying compensation."); Leary, *supra* note 8, at 1A.

[11] See discussion *infra* Parts III, IV.

[12] See discussion *infra* Parts III, IV. Other commentators have considered whether the conduct violates state and federal statutes specifically directed at prohibiting certain forms of computer activity. See Hale, *supra* note 7, at 544-52 (analyzing whether the conduct violates the Computer Fraud and Abuse Act of

1986 and the Electronic Communications Privacy Act); Kern, *supra* note 2, at 120-51 (analyzing whether the conduct violates the Computer Fraud and Abuse Act of 1986, the Electronic Communications Privacy Act, the Communications Act of 1934, and various state statutes prohibiting unauthorized access to computer systems). They have concluded that the conduct should not be viewed as violating these statutes. See Hale, *supra* note 7, at 544-52; Kern, *supra* note 2, at 120-51. This Article does not consider federal and state statutes that could arguably apply to the conduct. Rather, this Article considers only whether the common law applies.

[13] An analogous example of a neighbor harming the adjacent landowner but not violating any legally protected interest might occur if the neighbor were to construct an unsightly edifice which had a negative effect on surrounding property values. 66 C.J.S. Nuisances 32 (1998) ("[A] building or structure generally cannot be complained of as a nuisance merely because it interferes with the passage of light and air to adjoining premises, regardless of the impact on the injured party's property or person."); see also, e.g., *Sher v. Leiderman*, 226 Cal. Rptr. 698, 701-04 (Cal. Ct. App. 1986) (holding that landowners could not recover in tort against neighbor for harm caused to landowner's property in the form of sunlight blockage).

[14] See How and Why of WiFi, *supra* note 1.

[15] Energy that cannot be controlled cannot be possessed. See Black's Law Dictionary 1201 (8th ed. 2004) (defining "possession" to mean "the right under which one may exercise control over something to the exclusion of all others"). It is therefore incapable of being property. See Richard A. Epstein, Possession as the Root of Title, 13 Ga. L. Rev. 1221, 1222, 1238 (1979) (defending the common law proposition that "taking possession of unowned things is the only possible way to acquire ownership of them").

[16] See Epstein, *supra* note 15, at 1222 (commenting that the question of remedy for trespass is posterior to the question of whether a person holds a protected property right).

[17] See discussion *infra* section IV.A.

[18] See discussion *infra* section IV.A.

[19] See *Hickey v. Mich. Cent. R.R. Co.*, 55 N.W. 989, 990-91 (Mich. 1893); 66 C.J.S. Nuisances 87 (1998) ("It has been held that the person aggrieved may cut off branches of a neighbor's trees overhanging his land, remove a part of an adjoining owner's wall which overhangs his premises, or cut off the eaves of a building overhanging his property.").

[20] See discussion *infra* section IV.B.

[21] See Kern, *supra* note 2, at 108-09 (arguing on policy grounds that people should be permitted to access the Internet anywhere that Wi-Fi access points are available).

[22] Wi-Fi devices operate on the 2.4 and 5 GHz frequencies of the radio band. See How and Why of WiFi, *supra* note 1. The Federal Communications Commission ("FCC") has designated that users of these frequencies do not need a government-issued license. See generally 47 C.F.R. 15 (2004).

[23] See Kern, *supra* note 2, at 108-09.

[24] See, e.g., *e Bay, Inc. v. Bidder's Edge, Inc.*, 100 F. Supp. 2d 1058, 1069-72 (N.D. Cal. 2000) (ruling that plaintiff was entitled to preliminary injunctive relief because there was a strong likelihood that plaintiff would prevail at trial on a trespass to chattels claim based on defendant's use of plaintiff's website); *CompuServe, Inc. v. Cyber Promotions, Inc.*, 962 F. Supp. 1015, 1020-27 (S.D. Ohio 1997) (ruling that plaintiff was entitled to preliminary injunctive relief because there was a strong likelihood that plaintiff would prevail at trial on a trespass to chattels claim based on defendant's use of plaintiff's computer equipment to send unsolicited mass e-mails).

[25] *CompuServe*, 962 F. Supp. at 1021 ("Electronic signals generated and sent by computer have been held to be sufficiently physically tangible to support a trespass cause of action." (relying on *Thrifty-Tel, Inc. v. Bezenek*, 54 Cal. Rptr. 2d 468, 473 n.6 (Cal. Ct. App. 1996) (holding that electronic signals that defendants had generated to access a phone system were "sufficiently tangible to support a trespass cause of action"))).

[26] See *Bidder's Edge*, 100 F. Supp. 2d at 1069 ("It appears likely that the electronic signals sent by [the defendant] to retrieve information from eBay's computer system are also sufficiently tangible to support a trespass cause of action."); *CompuServe*, 962 F. Supp. at 1021-22.

[27] See How and Why of Wi-Fi, *supra* note 1.

[28] See discussion *infra* subsection III.B.1.

[29] See discussion *infra* subsection III.B.1.

[30] See discussion *infra* subsection III.B.2.

[31] See discussion *infra* subsection III.B.2.

[32] See Kern, *supra* note 2, at 110 (discussing the detrimental effect that free-riding users of a wireless network have on the capacity and infrastructure of an ISP).

[33] See discussion *infra* subsection III.B.2.

[34] See discussion *infra* subsection III.B.2.

[35] Kern, *supra* note 2, at 103.

[36] See How and Why of Wi-Fi, *supra* note 1.

[37] See Hewlett Packard, Introduction to Wireless, <http://h71036.www7.hp.com/hpp/cache/6588-0-0-225-121.html> (last visited May 15, 2006) (describing function of wireless router as a bridge that allows interconnectivity among computers that facilitates sharing of an Internet connection); Bradley Mitchell, Wireless Product Equipment-Network Routers, Access Points, Adapters and More, <http://compnetworking.about.com/od/wireless/ss/wirelessgear.htm> (last visited May 15, 2006) (explaining the role of wireless routers in a wireless network).

[38] See sources cited *supra* note 37.

[39] See sources cited *supra* note 37.

[40] The term "Bluetooth" represents a trade association, Bluetooth SIG, that has developed specifications for testing the quality of wireless devices. Bluetooth, Trademark Information, <http://www.bluetooth.com/Bluetooth/SIG/Trademark/> (last visited May 15, 2006). For a fee, Bluetooth will endorse devices that pass its quality test. Bluetooth, Membership Overview, <http://www.bluetooth.com/Bluetooth/SIG/Membership/> (last visited May 15, 2006). Examples of Bluetooth-endorsed products include keyboards, mice, palm pilots, and mobile phones. Bluetooth, Product Directory, <http://www.bluetooth.com/Bluetooth/Connect/Products/> (last visited May 15, 2006).

[41] Christopher W. Klaus, Wireless LAN 802.11b Security FAQ, http://www.iss.net/wireless/WLAN_Faq.php (last visited May 15, 2006) ("Cordless phones, baby monitors, and other devices like Bluetooth that operate on the 2.4 GHz frequency can disrupt a wireless network.").

[42] See Cisco Systems, Inc., Linksys White Papers: What Wireless Networking Means to Everyday People, at 7 (on file with author) [hereinafter Linksys White Paper].

[43] *Id.*

[44] *Id.* at 6-7.

[45] Kern, *supra* note 2, at 103. It is noteworthy that the 300-foot range of home wireless networks does not reflect the limits of technology. Using the proper antenna, a person could receive Wi-Fi radio signals as far away as a mile from the transmitting router. Wi-Fi Alliance, Range & Environment Issues, <http://wi-fi.org/OpenSection/range.asp?TIO=2> (last visited May 15, 2006); accord Hines, *supra* note 7 (stating that with a special amplification device, a person could receive Wi-Fi radio signals as far away as seventy-two miles).

[46] See Linksys White Paper, *supra* note 42, at 6-7.

[47] See Hale, *supra* note 7, at 543-44.

[48] Kern, *supra* note 2, at 104.

[49] See *id.* at 103; Linksys White Paper, *supra* note 42, at 6; Mitchell, *supra* note 37.

[50] See Jim Harrington, Linksys: Antenna Basics, (Nov. 19, 2001), at 2-6 (on file with author) (explaining how computer antennas function); Mitchell, *supra* note 37.

[51] See Hale, *supra* note 7, at 543.

[52] See *id.*

[53] See *id.* at 552-54.

[54] Kern, *supra* note 2, at 104.

[55] See Kumagai, *supra* note 8.

[56] This type of virus transmission is possible through a process called "port scanning." See Gary C. Kessler, Port Scanning: It's Not Just an Offensive Tool Anymore (May 2001), www.garykessler.net/library/ls_tools_scan.html. A computer connected to a network may contain a "port scanner" virus. A "port scanner" would probe the network, through the network's unique IP address, to determine which other computers are connected to that network. See *id.* After probing the network, the port scanner would search for software on the network computers vulnerable to virus attacks. See *id.*

[57] See Hines, *supra* note 7. It should be noted that a computer firewall that blocks virus transmission from sources on the Internet does not block viruses from sources within the network. See *id.* (advocating computer users purchase specialized firewalls for protection from virus dissemination within a network); Jeff Tyson, How Firewalls Work, <http://computer.howstuffworks.com/firewall.htm/printable> (last visited May 15, 2006) ("A firewall is simply a program or hardware device that filters the information coming through the Internet connection into your private network or computer system.").

[58] See Kern, *supra* note 2, at 104.

[59] Hale, *supra* note 7, at 554.

[60] *Id.* at 552-53.

[61] *Id.*

[62] See Kern, *supra* note 2, at 104. It should be noted that software programs exist which would enable a Wi-Fi operator to be aware of another person accessing the network. See, e.g., IBM Tivoli Monitoring, <http://www-306.ibm.com/software/tivoli/products/monitor/?CVM=ng> (last visited May 15, 2006) (describing network-monitoring software).

[63] See Kern, *supra* note 2, at 104.

[64] See Hale, *supra* note 7, at 546-47.

[65] In 2003, an estimated sixty-seven percent of Wi-Fi operators did not enable security measures. *Id.* at 547. By 2007, it is estimated that nearly eighty percent of wireless networks will be unsecured. *Id.*

[66] This Article does not consider whether joyriding gives rise to claims of trespass to land or nuisance. A brief analysis of these issues, however, reveals that neither tort applies. An argument that the joyriding neighbor commits a trespass to land relies on the premise that the Wi-Fi radio signals which the neighbor transmits to the Wi-Fi router constitute an actionable intrusion on the Wi-Fi operator's land. See Restatement of Torts 158 cmt. i, at 278 (1958) (stating that an actor may trespass to land by throwing, propelling, or placing a thing in the air space above the land). This premise is untenable because the radio signals operate on bandwidth frequencies that the FCC has designated as "unlicensed." See *supra* note 22. A person has no right to exclude another from using one of the unlicensed frequencies, even where the frequency lies within the geographic boundary of the person's land. For instance, the interference that a baby monitor causes to an adjacent landowner's cordless phone does not result in a trespass to land. With regard to the tort of nuisance, it is well established that federal law preempts a nuisance claim based on radio-signal interference. See *Brody v. Gotham Tower, Inc.*, 13 F.3d 994, 997-98 (5th Cir. 1994) (holding that enforcement of a nuisance claim based on radio-signal interference would contravene the doctrine of preemption, frustrating the objectives of the Federal Communications Act); *Goforth v. Smith*, 991 S.W.2d 579, 584-85 (Ark. 1999) (ruling that the FCC has exclusive jurisdiction over disputes involving radio-interference nuisance claims); *Still v. Michaels*, 803 P.2d 124, 124-25 (Ariz. 1990) (same); *Blackburn v. Doubleday Broad. Co.*, 353 N.W.2d 550, 555-57 (Minn. 1984) (same). Nuisance does not apply. With regard to the governing federal law, see *supra* note 12 and accompanying text.

[67] See Restatement of Torts 217, at 417.

[68] See Epstein, *supra* note 15, at 1222 (commenting that the question of remedy for trespass is posterior to the question of whether a person holds a protected property right).

[69] See *id.*

[70] See Kern, *supra* note 2, at 152 (considering the argument that a joyriding neighbor commits a trespass to chattel with respect to the Wi-Fi operator's "network"); Jason M. Kueser, Note, *This Lan Is My Lan, This Lan Is Your Lan: The Case for Extending Private Property Rights to Wireless Local Area Networks*, 22 UMKC L. Rev. 787, 797-98 (2004) (arguing that the radio signals that a wireless network transmits are property).

[71] Kueser, *supra* note 70, at 798. This argument stems from John Locke's labor theory of property. According to Locke, property rights vest when a person mixes his labor with a thing in a way "that excludes the common right of other Men." John Locke, *Two Treatises of Government* 306 (Peter Laslett ed., Cambridge Univ. Press 2d ed. 1967) (1690); see also William Blackstone, 2 Commentaries 405. In the Wi-Fi context, the data composing the Internet lie in public domain. Arguably, the Wi-Fi operator labors to sever transmissions of that data from the general commons by subscribing to an ISP service and by setting up a wireless network. Under Locke's theory, then, the Wi-Fi user's labor creates for the Wi-Fi user property rights in the wireless network.

[72] See discussion *supra* note 71.

[73] On three separate occasions, federal district courts have labeled a computer network as the subject of property. See *Am. Online, Inc. v. LCGM, Inc.*, 46 F. Supp. 2d 444, 452 (E.D. Va. 1998) ("The transmission of electrical signals through a computer network is sufficiently 'physical' contact to constitute a trespass to property.") (emphasis added); *Am. Online, Inc. v. IMS*, 24 F. Supp. 2d 548, 550 (E.D. Va. 1998); *Hotmail Corp. v. Van\$ Money Pie, Inc.*, No. C-98 JW PVT ENE, C 98-20064 JW, 1998 WL 388389, at 7 (N.D. Cal. Apr. 16, 1998) (opining that "computer networks" comprising an e-mail system can be personal property). As one commentator has noted, however, where courts have found aspects of computer accessing to be property, their analysis appears to have been driven by a results-oriented outcome. See Orlin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 28 N.Y.U. L. Rev. 1596, 1610-11 (2003).

[74] See, e.g., *Felst Publ'ns, Inc. v. Rural Tel. Serv. Co.*, 499 U.S. 340, 349 (1991) ("The primary objective of copyright is not to reward the labor of authors ...").

[75] 73 C.J.S. Property 7, at 9 (1998) ("It has been said that for a property right to exist in something, there must be an interest capable of a precise definition, it must be capable of exclusive possession or control, and the putative owner must have established a legitimate claim to exclusivity."); see also John E. Cribbet et al., Property 8 (David L. Shapiro et al. eds., The Foundation Press 1996) (1960) (commenting that exclusivity is a necessary criterion for an efficient system of property rights).

[76] For instance, property rights exist in intangible domain names because registration of a domain name excludes others from using it on the Internet. See *Kremen v. Cohen*, 337 F.3d 1024, 1030 (9th Cir. 2003).

[77] See How and Why of WiFi, *supra* note 1 (stating that wireless networks operate in the unlicensed 2.4 and 5 GHz bandwidths).

[78] An argument could be made that Wi-Fi radio signals can be contained within a physical boundary. A company called Force Field Wireless has developed, and sells, paint that, according to the company, bars the passage of radio signals. See Force Field Wireless, <http://www.forcefieldwireless.com/defendair.html> (last visited May 15, 2006). Apparently the paint is laced with copper and aluminum, both of which form an electromagnetic shield. Hines, *supra* note 7. Unfortunately the paint comes in only one color - gray. *Id.*

[79] See *supra* note 22.

[80] Linksys White Paper, *supra* note 42, at 6.

⁸¹ The fact that a wireless-device user cannot prohibit radio interference on an unlicensed frequency is consistent with the fact that a wireless-device user can prohibit a person from employing the frequency as a means to harm the user's personal property. The former fact concerns interference on the frequency bandwidth; the latter fact concerns personal property rights, independent of frequency interference.

⁸² This fact is also manifested by Congress's express declaration with respect to licensed frequencies. See 47 U.S.C. 301 (2000). But see Cribbet et al., supra note 75, at 9-10 (arguing that property rights exist in broadcast frequencies in at least economic terms). If in fact licensed frequencies cannot be owned, it appears certain that property rights do not attach to unlicensed frequencies either.

⁸³ See Linksys White Paper, supra note 42, at 6.

⁸⁴ Interference is "permissible" to the extent that the unlicensed frequencies are not regulated by government. See supra note 22.

⁸⁵ See sources cited supra note 37.

⁸⁶ William Shakespeare, Measure for Measure act 2, sc. 2.

⁸⁷ Kern, supra note 2, at 151; see also W. Page Keeton et al., Prosser and Keeton on the Law of Torts 14, at 85 (5th ed. 1984) (outlining the history of trespass to chattel and stating that it was employed in situations where animals were killed or beaten).

⁸⁸ See, e.g., Laura Quilter, The Continuing Expansion of Cyberspace Trespass to Chattels, 17 Berkeley Tech. L.J. 421, 435-36 (2002) (explaining that courts have employed the tort to deal with problems on the Internet); cases cited supra note 24.

⁸⁹ See, e.g., cases cited supra note 24.

⁹⁰ See Hale, supra note 7, at 552-55; Kern, supra note 2, at 151.

⁹¹ Restatement of Torts 217, at 417 (1958).

⁹² Id. 217 cmt. e, at 419.

⁹³ Id.

⁹⁴ Id.

⁹⁵ Id. 218 cmt. e, at 421-22.

⁹⁶ Id. 218, at 420.

⁹⁷ Id.

⁹⁸ Id. 218 cmt. e, at 421-22. Although an actor is not liable for harmless intermeddling, a chattel owner may use reasonable force to halt such intermeddling. Id.

⁹⁹ Radio signals are not material objects, but rather are electrical and magnetic fields. Harrington, supra note 50, at 2.

¹⁰⁰ See Restatement of Torts 217 cmt. e, at 419 (requiring physical contact for trespassory intermeddling); Kern, supra note 2, at 151-52 (stating that a trespass argument requires that the electronic signal be viewed as physical contact).

¹⁰¹ See, e.g., cases cited supra note 24.

¹⁰² See Am. Online, Inc. v. Nat'l Health Care Disc., 121 F. Supp. 2d 1255, 1259, 1277 (N.D. Iowa 2000); Am. Online, Inc. v. LCGM, 46 F. Supp. 2d 444, 451-52 (E.D. Va. 1998); Am. Online, Inc. v. IMS, 24 F. Supp. 2d 548, 550-51 (E.D. Va. 1998); CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1021-22 (S.D. Ohio 1997); Hotmail Corp. v. Van\$ Money Pie, Inc., No. C-98 JW PVT ENE, C 98-20064 JW, 1998 WL 388389, at 7 (N.D. Cal. Apr. 16, 1998).

¹⁰³ 962 F. Supp. 1015 (S.D. Ohio 1997).

¹⁰⁴ Id. at 1017.

¹⁰⁵ Id. at 1027.

¹⁰⁶ Id. at 1021. The CompuServe court relied on the reasoning of one case for this finding - a California State Court decision, Thrifty-Tel, Inc. v. Bezenek, 54 Cal. Rptr. 2d 468 (Cal. Ct. App. 1996). In Thrifty-Tel, children used software to conduct high-speed automated searches of possible access codes for a company's telephone system. Id. at 471-72. The court held that the children had committed a trespass to chattel. Id. at 473 n.6. According to the court, the electronic signals composing the access codes were "sufficiently tangible to support a trespass cause of action." Id. The court reached this conclusion by relying on cases holding that microscopic particles, such as dust and smoke, can constitute a trespass. Id. As one commentator has pointed out, however, those cases on which Thrifty-Tel relied dealt with trespass to land, not trespass to chattel. Dan L. Burk, The Trouble with Trespass, 4 J. Small & Emerging Bus. L. 27, 33 (2000).

¹⁰⁷ See, e.g., cases cited supra note 102.

¹⁰⁸ 24 F. Supp. 2d 548 (E.D. Va. 1998).

¹⁰⁹ *Id.* at 550.

¹¹⁰ 46 F. Supp. 2d 444 (E.D. Va. 1998).

¹¹¹ *Id.* at 552.

¹¹² See cases cited supra note 102.

¹¹³ E.g., *Am. Online, Inc. v. Nat'l Health Care Disc.*, 121 F. Supp. 2d 1255, 1259, 1277 (N.D. Iowa 2000).

¹¹⁴ See *Register.com, Inc. v. Verio, Inc.*, 126 F. Supp. 2d 238, 249-50 (S.D.N.Y. 2000); *e Bay, Inc. v. Bidder's Edge, Inc.*, 100 F. Supp. 2d 1059, 1069-72 (N.D. Cal. 2000).

¹¹⁵ 100 F. Supp. 2d 1059 (N.D. Cal. 2000).

¹¹⁶ *Id.* at 1060, 1062.

¹¹⁷ *Id.* at 1069.

¹¹⁸ See *id.*

¹¹⁹ 126 F. Supp. 2d 238 (S.D.N.Y. 2000).

¹²⁰ See *id.* at 245-50.

¹²¹ See *id.*

¹²² See *Bidder's Edge*, 100 F. Supp. 2d at 1069-72; *Am. Online, Inc. v. IMS*, 24 F. Supp. 2d 548, 550-51 (E.D. Va. 1998); *CompuServe, Inc. v. Cyber Promotions, Inc.*, 962 F. Supp. 1015, 1021-22 (S.D. Ohio 1997); *Hotmail Corp. v. Van\$ Money Pie, Inc.*, No. C-98 1W PVT ENE, C 98-20064 JW, 1998 WL 388389, at 7 (N.D. Cal. Apr. 16, 1998).

¹²³ See *Intel Corp. v. Hamidi*, 71 P.3d 296, 303-04 (Cal. 1996); *Ticketmaster Corp. v. Tickets.com, Inc.*, No. 99 CV7654, 2000 WL 1887522, at 4 (C.D. Cal. 2000). The courts in *Hamidi* and *Ticketmaster* declined to find a trespass to chattel on the basis that the electrical signal did not cause actionable harm. See *Hamidi*, 71 P.3d at 303-04; *Ticketmaster*, 2000 WL 1887522, at 4.

¹²⁴ See cases cited supra note 123.

¹²⁵ See Hewlett Packard, supra note 37 (describing function of wireless router).

¹²⁶ See Burk, supra note 106, at 32-34.

¹²⁷ See Harrington, supra note 50, at 2.

¹²⁸ See *id.*

¹²⁹ Burk, supra note 106, at 32-34.

¹³⁰ *Id.* at 34.

¹³¹ *Id.*

¹³² *Id.*

¹³³ See Restatement of Torts 217, at 417, 218 cmt. e, at 421-22 (1958); see also discussion supra section III.B.

¹³⁴ See *Chair King, Inc. v. GTE Mobilingt of Houston, Inc.*, 135 S.W.3d 365, 395 (Tex. App. 2004) (refusing to recognize that an unsolicited fax resulted in a trespass to chattel because the fax recipient sustained no actual damages).

It is noteworthy that even an obscenely offensive telephone call would not satisfy the harm requirement for trespass to chattel. See *Intel Corp. v. Hamidi*, 71 P.3d 296, 308-09 (Cal. 1996) (rejecting argument that electrical signal can harm recipient based on the content of the message sent via the signal).

¹³⁵ See Restatement of Torts 218 cmt. e, at 421-22; W. Page Keeton et al., supra note 87, 14, at 87. It should be noted that in circumstances where an actor touches but does not harm a chattel, the chattel owner may use reasonable force to halt the touching. Restatement of Torts 218 cmt. e, at 421-22. For example, a car owner may remove a person who refuses to move from the owner's car. W. Page Keeton et al., supra note 87, 14, at 87. In the context of electronic signals, then, a telephone owner may use reasonable force to protect her phone from the electronic signals of an unwanted telephone call—she may hang up on the caller.

¹³⁶ Restatement of Torts 217, at 417.

¹³⁷ *Id.* cmt. c, at 418.

¹³⁸ See id.

¹³⁹ See id. at 417.

¹⁴⁰ See W. Page Keeton et al., *supra* note 87, 14, at 87 (noting that patting a horse does not result in trespass to chattel).

¹⁴¹ Restatement of Torts 217, at 417, 218 cmt. e, at 421-22.

¹⁴² Id. 218, at 420; see also W. Page Keeton et al., *supra* note 87, 14, at 87 (observing that harmless interference will not result in a trespass to chattel).

¹⁴³ Restatement of Torts 218 cmt. e, at 421-22.

¹⁴⁴ It is arguable that the neighbor unintentionally commits other harms against the Wi-Fi operator. The Wi-Fi operator could be liable to an ISP for permitting a third party to access the ISP's services without authorization. See Kerr, *supra* note 73, at 1599-1600, 1637-39 (observing that courts have interpreted "unauthorized access" as occurring when a computer user accesses another's computer network in violation of a contract between that other person and a third party). In most contractual agreements with ISPs, Wi-Fi operators agree to restrict their use of the ISP's services. Hale, *supra* note 7, at 555. For instance, one ISP service agreement states that that user agrees "not to permit anyone else to use [the] Member Account." See SBC Yahoo! Terms of Service, <http://sbc.yahoo.com/terms/> (last visited May 15, 2006). By failing to password protect the wireless network, the Wi-Fi operator who fails to institute security measures is arguably permitting anyone within the physical range of the network's range to access the ISP's services. The Wi-Fi operator could therefore be breaching the ISP agreement if that agreement specifically restricts the usage of ISP services to the Wi-Fi operator. Such a breach would likely impair the value of the router: the router would be the means by which the Wi-Fi operator becomes liable to the ISP, so its value would decrease in proportion to the amount of liability. A harm arguably results.

Despite the presence of this harm, it is not likely actionable under trespass to chattel because it is economic in nature. Courts have refused to recognize economic harm as a basis for supporting liability under a claim of trespass to chattel. See *Intel Corp. v. Hamidi*, 71 P.3d 296, 309 (Cal. 2003) (refusing to recognize "consequential economic damages" as satisfying the requirement for harm under trespass to chattel).

Another harm could occur based on the fact that every website that a joyriding neighbor visits will register the Wi-Fi operator's unique IP address. See Hines, *supra* note 7. Tracing which Internet users visited particular websites could potentially harm the reputation of the Wi-Fi operator, especially given that downloading child pornography through another person's Wi-Fi connection has become a reality. See id.; Seth Schiesel, Growth of Wireless Internet Opens New Path for Thieves, N.Y. Times, Mar. 19, 2005, at A1. It is possible, then, that a Wi-Fi operator could suffer reputational harm due to the neighbor's joyriding.

¹⁴⁵ See Hines, *supra* note 7 (reporting that joyriding can result in a decrease in Internet performance for a Wi-Fi operator).

¹⁴⁶ Hale, *supra* note 7, at 552; Hines, *supra* note 7.

¹⁴⁷ Hale, *supra* note 7, at 553.

¹⁴⁸ Id. at 552-53; Hines, *supra* note 7. Admittedly, not all instances of joyriding result in this first harm. Checking e-mail or viewing websites would not noticeably slow down the rate of data transmission. See Hale, *supra* note 7, at 554.

¹⁴⁹ See Klaus, *supra* note 41 ("Next generation virus and worms have become a multi-vector attack programs [sic] that self-propagate through any TCP/IP interface including wireless. If one computer on a wireless network is infected with a hybrid threat, this threat can easily spread to other wireless computers and potentially internal computers behind the wireless network."); see also Kumagai, *supra* note 8.

The opposite situation - where the joyriding neighbor receives a virus from the Wi-Fi operator - would not give rise to a tort action against the Wi-Fi operator. Presumably the joyriding neighbor would bring a negligence suit against the Wi-Fi operator for breaching a duty of care to operate the network without any harmful computer viruses. See W. Page Keeton et al., *supra* note 87, 30, at 164-65 (outlining the elements of a negligence cause of action). The Wi-Fi operator would likely be viewed as having assumed the risk of harm by logging onto the wireless network. See id. 68, at 484-85 (explaining the considerations in finding an implied assumption of risk). Likely the situation would be analogous to a property owner who allows his bumble bees to fly onto land where the bees consume poison. See *Jeanes v. Holt*, 211 P.2d 925, 927 (Cal. Dist. Ct. App. 1949) (ruling that defendant was not negligent where neighbor's bees came onto defendant's land and consumed poisonous fertilizer). Just as the landowner would not be liable for negligently killing the bees, so also would the Wi-Fi operator not be liable for negligently spreading a computer virus. See id.

¹⁵⁰ See Klaus, *supra* note 41; see generally discussion *supra* note 56.

¹⁵¹ See Klaus, *supra* note 41; Kumagai, *supra* note 8; Linksys White Paper, *supra* note 42.

¹⁵² Protecting a computer from receiving a virus through a local network requires a unique type of computer firewall that is unlike a firewall designed to protect against viruses received through the Internet. See Hines, *supra* note 7 (encouraging Wi-Fi users to institute firewalls specifically designed for protecting viruses from spreading among network users); Tyson, *supra* note 57 ("A firewall is simply a program or hardware device that filters the information coming through the Internet connection into your private network or computer system.").

¹⁵³ Restatement of Tort 218, at 420 (1958).

¹⁵⁴ Id. 218 cmt. h, at 422.

¹⁵⁵ See Curt Franklin, How Routers Work, <http://computer.howstuffworks.com/router.htm/printable> (last visited May 15, 2006) (explaining the operations of a router).

¹⁵⁶ See id.

¹⁵⁷ See Marshall Brain, How Computer Viruses Work, <http://computer.howstuffworks.com/virus.htm/printable> (last visited May 15, 2006) (noting that computer viruses can harm files on a computer machine).

¹⁵⁸ See id.

¹⁵⁹ See Restatement of Torts 218(c) & cmt. 1, at 420, 423 (stating that harmful contact may occur where the chattel owner is deprived of the chattel's use).

¹⁶⁰ Id. The argument against finding a trespass because no physical impairment is present is also flawed for another reason. Physical impairment is not absolutely required for an intermeddling to be actionable. According to the Restatement, it is possible that "the value to the owner of a particular type of chattel may be impaired by dealing with it in a manner that does not affect its physical condition." Id. 218 cmt. h, at 422. For instance, a person who wears another's lingerie, or who brushes the person's own teeth with another's toothbrush, commits a trespass to chattel even though the chattel remains physically unimpaired. Id. The lingerie and toothbrush owner could sell their respective chattels for the same price as they could before the actor intermeddled with the chattels, yet from their standpoint, the their chattels have decreased in value. Value arises from the fact that no one else makes use of them, even though the chattels function properly. Although the router is not the same sort of chattel as lingerie or a toothbrush, it seems that value lies in the fact that the neighbor does not joyride on the router. Under the lingerie-toothbrush rationale, a court could find that the neighbor's intermeddling is trespassory without finding that physical contact occurred. See Id.

¹⁶¹ See id. 218 cmt. i, at 423.

¹⁶² Id. Illus. 4.

¹⁶³ See id.

¹⁶⁴ Id. 218 cmt. i, at 423 ("The deprivation of use, not amounting to a dispossession, necessary to render the actor liable for his use or other intermeddling with the chattel of another without the other's consent must be for a time so substantial that it is possible to estimate the loss caused thereby.").

¹⁶⁵ See Cribbet et al., *supra* note 75, at 2 ("It appears, then, that 'ownership' consists of many disparate claims [with respect to one chattel] sanctioned by law against many persons - a 'bundle of sticks,' as legal scholars sometimes have put it.").

¹⁶⁶ See W. Page Keeton et al., *supra* note 87, 14, at 85-86 (describing trespass to chattel as interferences "which are not sufficiently important to be classed as conversion").

¹⁶⁷ See id.

¹⁶⁸ Id.

¹⁶⁹ See id.; e Bay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1071 (N.D. Cal. 2000) (finding harm based on the fact that defendant had deprived plaintiff "of the ability to use [a] portion of its personal property for its own purposes") (emphasis added).

¹⁷⁰ The point that not every use must be disabled for a trespass to occur is illustrated by the following example. Consider someone who intentionally disengages a spark plug from another's car so that the car performs poorly. The car is not permanently damaged by disengaging the spark plug. The car owner can still speed on a highway, open the sunroof, listen to its radio, stop at a light, and perform nearly every other use of the car. Nevertheless, the car owner cannot run the engine at its most efficient level in the absence of the spark plug. That is, the car owner cannot realize one possible use of the car - driving the car with all spark plugs. During the time that the spark plug is disengaged, the car owner is deprived of making full use of the car. The value temporarily decreases. Trespass to chattel lies.

¹⁷¹ See discussion *supra* subsection III.B.2.a.

¹⁷² Hale, *supra* note 7, at 554.

¹⁷³ Id.

¹⁷⁴ See Restatement of Torts 218 cmt. e, at 421-22 (1958).

¹⁷⁵ See e Bay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1071 (N.D. Cal. 2000) (ruling that harm resulted from defendant's searches of a website even where the searches constituted "a negligible load on plaintiff's computer systems"); Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238, 249-50 (S.D.N.Y. 2000) (same); Am. Online, Inc. v. IMS, 24 F. Supp. 2d 548, 550 (E.D. Va. 1998) (finding actionable harm based on an injury to goodwill); CompuServe, Inc. v. Cyber Promotions, Inc., 952 F. Supp. 1015, 1022 (S.D. Ohio 1997) (commenting that the defendant's use of ISP's disk space and processing power when the defendant sent an e-mail).

¹⁷⁶ See cases cited *supra* note 175; cf. Restatement of Torts 218 cmt. e, at 421-22 (requiring harm for trespass to chattel to lie).

¹⁷⁷ Bidder's Edge, 100 F. Supp. 2d at 1071.

¹⁷⁸ Id. at 1064.

¹⁷⁹ See id. at 1071 (discounting defendant's argument that website searches represented "a negligible load on plaintiff's computer systems" because the searches deprived plaintiff of an ability to use a portion of personal property).

¹⁸⁰ Id. (emphasis added).

¹⁸¹ Id. at 1066, 1071. The court attempted to portray its discourse on harm as consistent with trespass jurisprudence. See id. at 1071. The flaw in its reasoning is apparent, however. Initially, the court relied on the true premise that the law does not recognize a right to commit a harmless intermeddling. Id. From that premise, the court faultily concluded that harmless intermeddling is actionable. Id. The fact that the law does not recognize a right to commit harmless intermeddling does not imply that the law condemns harmless intermeddling. Despite the court's ostensible attempt to cram its holding into the well established jurisprudence of tort law, it failed. The court introduced an exception to the rule - not a consistency.

¹⁸² Id. at 1066, 1071.

¹⁸³ Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238, 243-44, 248-50 (S.D.N.Y. 2000).

¹⁸⁴ Id. at 249-50.

¹⁸⁵ Id. at 250.

¹⁸⁶ CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1022 (S.D. Ohio 1997).

¹⁸⁷ See id. at 1022.

¹⁸⁸ See Marshall Brain, How E-Mail Works, <http://computer.howstuffworks.com/email.htm/printable> (last visited May 15, 2006).

¹⁸⁹ See CompuServe, 962 F. Supp. at 1022.

¹⁹⁰ See cases cited supra note 175.

¹⁹¹ See e Bay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1066 (N.D. Cal. 2000) ("If [defendant's] activity is allowed to continue unchecked, it would encourage other auction aggregators to engage in similar recursive searching of the eBay system such that eBay would suffer irreparable harm from reduced system performance, system unavailability, or data losses.").

¹⁹² 71 P.3d 296 (Cal. 2003).

¹⁹³ Id. at 299-300.

¹⁹⁴ Id. at 303-04.

¹⁹⁵ Id. at 304-06.

¹⁹⁶ See id.

¹⁹⁷ Id. at 307-08.

¹⁹⁸ Id. at 299-300.

¹⁹⁹ Id. at 300.

²⁰⁰ See id.

²⁰¹ See id.

²⁰² See cases cited supra note 175.

²⁰³ See Hamidi, 71 P.3d at 300.

²⁰⁴ Hale, supra note 7, at 547.

²⁰⁵ See cases cited supra note 175.

²⁰⁶ See Quilter, supra note 88, at 435-36 (arguing that courts have incorrectly applied trespass to chattel to deal with public annoyances on the Internet).

²⁰⁷ See Daniel Dern, Meeting the Challenges of Business and End-User Communities on the Internet: What They Want, What They Need, What They're Doing, in Public Access to the Internet 212-13 (Brian Kahin & James Keller eds., 1996) (explaining, at the time that the Internet was initially becoming commercial, that commercial Internet users seek "accountability and clear problem-resolution paths").

²⁰⁸ See, e.g., e Bay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1066-72 (N.D. Cal. 2000).

²⁰⁹ This conclusion seems likely given that the neighbor must purchase a wireless network adapter to interface with the wireless network. See discussion supra Part II. A wireless network adapter costs approximately seventy dollars. See Best Buy, <http://www.bestbuy.com/site/olspage.jsp?navLevel=4&type=category&navHistory=cat00000%2Bcat01000%2Bcat01024&id=cat01032> (last visited Jan. 6, 2006) (displaying retail of price of 802.11g Wireless Notebook Card to be \$ 70.99).

²¹⁰ Kern, supra note 2, at 110 (discussing the detrimental effect that free-riding users of a wireless network have on the capacity and infrastructure of an ISP).

²¹¹ See Bidder's Edge, 100 F. Supp. 2d at 1066 ("If [defendant's] activity is allowed to continue unchecked, it would encourage other auction aggregators to engage in similar recursive searching of the eBay system such that eBay would suffer irreparable harm from reduced system performance, system unavailability, or data losses.").

²¹² See cases cited supra note 175.

213 Restatement of Torts 217 cmt. c, at 418 (1958).

214 See *id.*

215 See cases cited supra note 175.

216 A third point is also noteworthy. The intent requirement distinguishes the neighbor's tortious conduct from the harmless conduct of other wireless-device users. See discussion *supra* subsection III.B.1.b (discussing the distinction between electrical devices that cause harmless intermeddling and those which do not). No cause of action lies against parents who operate baby monitors that happen to interfere with the performance of another's Wi-Fi router. See Restatement of Torts 217 cmt. c, at 418. Nor is there a cause of action against cordless phone users. See *id.* Presumably, a person who uses these wireless devices does not intend to intermeddle with another person's use of a wireless device.

217 See Restatement of Torts 217 cmt. c, at 418 ("It is immaterial that the actor Intermeddles with the chattel under a mistake of law or fact that the possessor has consented to his dealing with it.").

218 ¶ Id.

219 See *id.* It should be noted that one commentator has voiced a contrary view. See Kern, *supra* note 2, at 155. Without relying on any authority, he states: "The intent component of [trespass to chattel] requires that a roaming [Wi-Fi] user knew or was reckless as to whether his or her access would cause a disruption on the operator's service." *Id.* This statement contravenes the express dictate of the general rule set forth in the Restatement. See *Restatement of Torts* 217 *cm.* c, at 418.

220 See Restatement of Torts 217 cmt. c, at 418. ("An intention is present when an act is done for the purpose of using or otherwise intermeddling with a chattel ...").

221 See discussion *infra* section IV.A.

222 See discussion *Infra* section IV.B.

223 See Restatement of Torts 892A, at 364 ("One who effectively consents to conduct of another intended to invade his interests cannot recover in an action of tort for the conduct or for harm resulting from it.").

224 Id. 892, at 362 ("[Consent] may be manifested by action or inaction and need not be communicated to the actor.").

225 Id. 892 cmt. c, at 363 (explaining "apparent consent").

226 See *EF Cultural Travel BV v. Zefer Corp.*, 318 F.3d 58, 62-63 (1st Cir. 2003); e *Bay, Inc. v. Bidder's Edge, Inc.*, 100 F. Supp. 2d 1058, 1070 (N.D. Cal. 2000); *CompuServe, Inc. v. Cyber Promotions, Inc.*, 962 F. Supp. 1015, 1023-24 (S.D. Ohio 1997).

2277 318 F.3d 58, 60, 62-63 (1st Cir. 2003).

228* Id. at 60, 62-63.

229 ² Id. at 63. The court actually held that the owner had "authorized" the conduct, rather than "consented" to the conduct. Id.

230 Id. ("Password protection itself normally limits authorization by implication (and technology), even without express terms.")

231 * CompuServe, 962 F. Supp. at 1023-24.

232 *Id.* at 1023.

233 7 Id. at 1023-24.

2347 e Bay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1070 (N.D. Cal. 2000).

235 F. Id.

236 Id. at 1060, 1070.

237 See *id.*

238 See *id.* This fact also influenced the court in *EF Cultural Travel BV v. Zefer Corp.*, 318 F.3d 53, 63 (1st Cir. 2003).

239 See Zefer, 318 F.3d at 63.

240 See *CompuServe, Inc. v. Cyber Promotions, Inc.*, 962 F. Supp. 1015, 1023-24 (S.D. Ohio 1997).

241 See *id.*

²⁴² See *Bidder's Edge*, 100 F. Supp. at 1070.

²⁴³ See Kern, *supra* note 2, at 155-56.

²⁴⁴ See *Zefer*, 318 F.3d at 63.

²⁴⁵ See Kern, *supra* note 2, at 156 ("It is not clear that a court would use [the same test for consent as in the website trespass cases] with respect to a roaming Wi-Fi user because a wireless network may in some cases have more of a private character than a website.").

²⁴⁶ See, e.g., NetZero ISP, <http://www.netzero.com> (last visited May 15, 2006) (offering e-mail service as a benefit for Internet users who pay the ISP a fixed monthly fee).

²⁴⁷ See, e.g., Earthlink ISP, <http://www.earthlink.net/membercenter/benefits/> (last visited May 15, 2006) (listing the ability to exchange e-mail as a benefit that Internet users realize when subscribing to the ISP service).

²⁴⁸ This fact is evidenced by the growing business of website advertising. See, e.g., Search Engine Wizards, <http://www.searchenginewizards.com> (last visited May 15, 2006) ("Using effective search engine solutions, companies can add new revenue streams that were previously unavailable."); Multimedia Advertising Services, Inc., <http://www.masresults.com/advertising.htm> (last visited May 15, 2006) (selling a website marketing service).

²⁴⁹ See sources cited *supra* notes 246-48.

²⁵⁰ See *Gates v. Navy*, 617 S.E.2d 163, 167 (Ga. App. 2005) ("It is well-settled that the defenses of ... assumption of the risk and contributory negligence are not valid defenses to intentional, wilful, or wanton and reckless torts ...") (internal citations omitted); see generally W. Page Keeton et al., *supra* note 87, 68, at 480-98 (discussing assumption of risk in context of negligence defenses).

²⁵¹ See discussion *supra* Part III.

²⁵² *Gates*, 617 S.E.2d at 167; see also W. Page Keeton et al., *supra* note 87, 18, at 113 ("The mere fact that one is willing to incur a risk that conduct in deliberate violation of the rules of a sporting contest will be committed does not mean that one is willing for such conduct to be committed.").

²⁵³ *Gates*, 617 S.E.2d at 167.

²⁵⁴ See *id.*

²⁵⁵ The bull-in-the-china-shop example is by no means completely analogous to the Wi-Fi scenario under consideration. The narrative is cited only for the general proposition that assumption of risk is no defense to an intentional tort, and nothing more than that. Unlike the bull owner, the joyriding neighbor presumably does not intentionally slow down the router or transmit a virus through the router. That difference does not detract from the inference drawn from the bull narrative: assumption of risk is not a defense to an intentional tort.

²⁵⁶ See *Kelly v. Cook*, 73 So. 220, 221 (Ala. Ct. App. 1916) ("The evidence shows that this cotton was taken in the absence of the plaintiff and delivered to the defendant without her knowledge; and the mere silence of the plaintiff after knowledge of the conversion was brought to her did not amount to a ratification of the taking or a waiver of the tort.").

²⁵⁷ See *id.*; W. Page Keeton et al., *supra* note 87, 18, at 119-20 (commenting that consent is not a defense to tortious conduct where the seeming consent is provided without full knowledge of the nature and quality of the conduct).

²⁵⁸ Cf. Patricia L. Bellia, *Defending Cyberproperty*, 79 N.Y.U. L. Rev. 2164, 2272-73 (2004) (arguing that trespass to chattel should arise in the computer-network context only if the network operator has implemented actual notice of conditions for access to the network).

²⁵⁹ See W. Page Keeton et al., *supra* note 87, 18, at 113 ("Silence and inaction may manifest consent where a reasonable person would speak if he objected.") (emphasis added).

²⁶⁰ See *id.*

²⁶¹ See Restatement of Torts 264, at 498 (1958) ("One is privileged to commit an act which would otherwise be a trespass to the chattel of another or a conversion of it, for the purpose of abating a private nuisance created or maintained by the other, if the act is a reasonable means of abating the nuisance, and if the other upon demand has failed to abate the nuisance, or the actor reasonably believes that such demand is impractical or useless.").

²⁶² *Id.*

²⁶³ *Id.* 821D, at 100 ("A private nuisance is a nontrespassory invasion of another's interest in the private use and enjoyment of land.").

²⁶⁴ 66 C.J.S. Nuisances 89, at 635 (1998).

²⁶⁵ *Hickey v. Mich. Cent. R.R. Co.*, 55 N.W. 989, 990-91 (Mich. 1893); see also 66 C.J.S. Nuisances 87, at 634 ("It has been held that the person aggrieved may cut off branches of a neighbor's trees overhanging his land, remove a part of an adjoining owner's wall which overhangs his premises, or cut off the eaves of a building overhanging his property.").

²⁶⁶ See Klaus, *supra* note 41; Linksys White Paper, *supra* note 42, at 6.

²⁶⁷ See Restatement of Torts 264, at 498 (outlining the abatement-of-nuisance defense to trespass to chattel).

²⁶⁸ See *Browde v. Gotham Tower, Inc.*, 13 F.3d 994, 997-98 (6th Cir. 1994) (holding that enforcement of a nuisance claim based on radio-signal interference would contravene the doctrine of preemption, frustrating the objectives of the FCA); *GoForth v. Smith*, 991 S.W.2d 579, 584-85 (Ark. 1999) (ruling that the FCC has exclusive jurisdiction over disputes involving radio-interference nuisance claims); *Still v. Michaels*, 803 P.2d 124, 124-25 (Ariz. Ct. App. 1990) (same); *Blackburn v. Doubleday Broad. Co.*, 353 N.W.2d 550, 555-57 (Minn. 1984) (same).

²⁶⁹ See 47 U.S.C. 333 (2000) (prohibiting interference with radio communications on licensed frequencies only).

²⁷⁰ The FCA grants the FCC authority to regulate bandwidths. See *id.* 303. A requirement for operating a device on unlicensed frequencies is that the operator must accept interference. See 47 C.F.R. 15.5(b) (2004). Thus, insofar as a device satisfies technical specifications, the FCC appears to permit interference that such devices may cause within the unlicensed bandwidth. See 47 U.S.C. 333; Ellen P. Goodman, Spectrum Rights in the Telecosm To Come, 41 San Diego L. Rev. 269, 287-88 (2004) ("The FCC has opened the bands for low-power transmissions by operators or members of the public without mandating licensing or coordination. The only requirement is that the equipment used in these unlicensed bands must satisfy certain technical specifications.").

²⁷¹ 66 C.J.S. Nuisances 89, at 635 (1998).

²⁷² *Id.*

²⁷³ See *id.*

²⁷⁴ See Hewlett Packard, Wi-Fi and Bluetooth--Interference Issues, at 1 (Jan. 2002), available at <http://www.hp.com/rnd/library/pdf/WiFiBluetoothcoexistence.pdf> ("Only in extreme conditions, such as setting a Bluetooth-enabled cell phone down next to an operating microwave oven, is it likely that communications will cease altogether.").

²⁷⁵ *Id.* at 2 ("There can be no more than three different Wi-Fi networks operating in close proximity to one another.").

²⁷⁶ *Id.*

²⁷⁷ See 66 C.J.S. Nuisances 89, at 635 (stating that abatement is permissible only in instances of "extreme" or "urgent" necessity).

²⁷⁸ See *id.*

²⁷⁹ Assuming *arguendo* that these facts did exist, joyriding does not appear a reasonable means for abating the nuisance. To be excused for an action of trespass, an actor must reasonably believe that a demand on the chattel owner to cease the nuisance would be impractical or useless. Restatement of Torts 264, at 498 (1958). A more reasonable method of abatement would be for the neighbor simply to request that the Wi-Fi operator either physically relocate or cease using any one of the many wireless devices creating the shortage. Given that the Wi-Fi operator prefers that the neighbor not joyride, the Wi-Fi operator would likely acquiesce to such a request. This method of abatement - the simple request - appears more reasonable than joyriding because it would not subject the Wi-Fi operator to the potential harms discussed above. See discussion *supra* subsection III.B.2.

²⁸⁰ See discussion *supra* section III.A.

²⁸¹ See discussion *supra* subsection III.B.1.

²⁸² See discussion *supra* subsection III.B.3.

²⁸³ See discussion *supra* subsection III.B.2.a.

²⁸⁴ See discussion *supra* subsection III.B.2.a.

²⁸⁵ See discussion *supra* subsection III.B.2.b.

²⁸⁶ See cases cited *supra* note 175.

²⁸⁷ See discussion *supra* subsection III.B.2.b.

²⁸⁸ See discussion *supra* Part IV.

²⁸⁹ See discussion *supra* section IV.A.

²⁹⁰ See discussion *supra* section IV.A.

²⁹¹ See discussion *supra* section IV.A.

²⁹² See discussion *supra* section IV.A.

²⁹³ See discussion *supra* section IV.A.

²⁹⁴ See discussion *supra* section IV.A.

²⁹⁵ See discussion *supra* section IV.A.

7/7/2015

ARTICLE: Accessing the Internet Through the Neighbor's Wireless Internet Connection: Physical Trespass in Virtual Reality, 84 Neb. L. Rev. 1226

[296 ¶](#) See discussion supra section IV.A.

[297 ¶](#) See discussion supra section IV.B.

[298 ¶](#) See discussion supra section IV.B.

[299 ¶](#) See discussion supra section IV.B.

[300 ¶](#) See cases cited supra note 268.

[301 ¶](#) See 66 C.J.S. Nuisances 89, at 635 (1998).

[302 ¶](#) See discussion supra section IV.B.

Jump To ▾



LexisNexis

COMMONWEALTH OF MASSACHUSETTS

APPEALS COURT

NO. 2015-P-0558

COMMONWEALTH

V.

ADALBERTO MARTINEZ

ON APPEAL FROM A JUDGMENT OF
THE FALL RIVER DISTRICT COURT

BRIEF
OF THE DEFENDANT

BRISTOL, SS.